RISK MANAGEMENT POLICY AND FRAMEWORK

March 2018

Table of contents

1 Risk management context **1**

2 Risk management framework terminology **1**

3 Risk policy and interpretation **3**

3.1 Policy 3

3.2 Policy interpretation: What this means for you 3

3.3 Risk management accountabilities 4

4 What is the risk management process? **7**

4.1 Risk process initiation and context 9

4.2 Risk identification 9

4.3 Risk analysis 10

4.4 Risk evaluation 10

4.5 Risk management and treatment 10

4.6 Risk reporting 11

4.7 What is risk materiality? 11

4.8 What are the risk categories? 12

4.9 Analysis of risks 12

4.10 What is the Risk Register? 14

4.11 What is the risk tolerance threshold matrix? 14

4.12 What is the risk dashboard? 14

5 Document control **14**

Attachment 1: Risk Register example **15**

Attachment 2: Risk tolerance threshold matrix **16**

1 Risk management context

The Natural Resources Commission (the Commission) provides independent advice to the NSW Government on managing the state's natural resources. The Commission's mission is to provide evidenced based advice in a complex and uncertain operating environment.

Enterprise Risk Management (ERM) is a comprehensive, systematic approach to help the Commission to identify risk events and states, and measure, prioritise and respond to the risks challenging our projects and activities.

Successful organisations are good at managing risk. The Commission has adopted a consistent enterprise wide approach that builds internal risk management competencies and ensures that staff can respond effectively to risk data. Making risk consideration as a part of decision making at all levels within the Commission is an essential element of enterprise-wide risk management.

The value offered by ERM is illustrated in **Figure 1**.

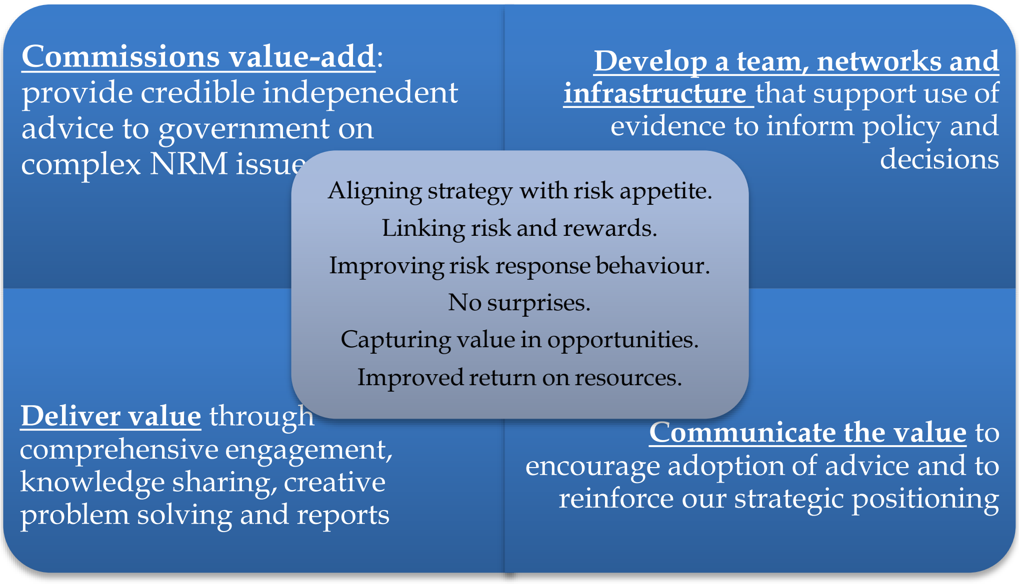

Figure 1: Relationship of risk management value to the Commission's objectives

This document establishes the framework that integrates the process of risk management into the Commission's overall governance, management, reporting, policies, and culture. It explains the policy and approach used to identify and manage its risks.

The Commission's Shared Audit and Risk Committee 'Charter' and the 'Risk Policy' provide the enterprise risk management framework, and have been developed in accordance with the Risk Management Standard AS/NZS ISO 31000:2009 (ISO 31000); NSW Treasury TPP 15-03; and the Commission's Governance Policy (D12/4558). The development of the risk framework has also been informed by commercial best practice, appropriate to the scale and operations of the Commission.

2 Risk management framework terminology

Consequence	The outcome of a risk if it occurs. Threats have unfavourable consequences, and opportunities have favourable consequences. Consequences can be expressed

	either quantitatively or qualitatively.
Control	A measure or action applied to modify the likelihood and / or consequence of a risk event or condition occurring. May include any process, policy, practice or actions which modify risk.
Inherent risk	The risk and consequence as originally identified before controls and treatments are implemented
Likelihood	The chance that a risk event will occur. Expressed as either a single event probability, or repeat event frequency.
Material business risk	Risks are material business risks if they have a material effect on the operations or survivability of the organisation as a whole, or will materially affect its key stakeholders.
Opportunity	A positive risk: an uncertain beneficial event or state that will result in favourable outcomes if it occurs, e.g. enhanced reputation, new high value work, improved stakeholder outcomes.
Residual risk	The risk remaining or retained after agreed treatments are implemented.
Risk acceptance threshold	The agreed level of risk exposure above which increased controls, and resources are required to manage the risk, with increasing pro-activity; and below which risks may be accepted.
Risk appetite	The level of risk exposure which is considered tolerable and justifiable should it be realised; i.e. below the acceptance threshold.
Risk analysis	The consideration of the causes and sources of risks, their positive and negative consequences, and the likelihood those consequences will occur
Risk assessment	The overall process of risk identification, analysis and evaluation
Risk evaluation	The process of estimating the likelihood and consequence of identified risks, and assessment against defined risk acceptance thresholds.
Risk identification	A structured process to identify and disclose threats and opportunities that may be encountered in pursuing business activity.
Risk management	The culture, processes, structures and decisions that are directed towards realising potential opportunities while managing adverse effects.
Risk profile	The documented and prioritised overall assessment of the range of specific risks faced by the Commission
Threat	A negative risk; an uncertain adverse event or condition that if it occurs will result in unfavourable outcomes. This could include for example injury, environmental or physical infrastructure damage, economic loss to communities, or loss of stakeholder confidence in or damage to the Commission's reputation.
Treatment	A process to modify risk exposure, that can involve avoiding, taking or retaining the risk; or that implements controls that mitigate, transfer, or share the risk.

3 Risk policy and interpretation

3.1 Policy

Risk is the influence of uncertainty on the Commission agency objectives, its people, assets and operational activities. The Commission recognises that risk is an integral component of our working environment that is characterised by both opportunity and threat to the organisation.

The risk appetite is defined under two specific areas; corporate and advice based. The corporate willingness to accept risk can be defined as low, whilst the willingness to accept risk that is related to independent advice can be high, particularly when the advice is designed to encourage reform and change.

A risk aware culture will assist to manage risk appropriately, enabling us to make informed business decisions to realise potential gains whilst avoiding or limiting negative effects or outcomes.

The effective management of risk is vital to the Commission's success. Being alert to risk, behaving with discipline in risk disclosure, and implementing appropriate risk controls and accountabilities are all essential to deliver acceptable risk outcomes. Therefore, an enterprise risk management framework is maintained to ensure the Commission:

- regularly reviews and sets acceptable risk tolerance thresholds and risk categories, appropriate delegations of risk authority, and approves the Charter for the Shared Audit & Risk Committee
- has a risk management framework, appropriate to its scale and operations
- identifies and monitors material business risks, takes immediate corrective action to manage these risks within acceptable tolerance levels
- regularly reports identified material business risks, and the status and effectiveness of risk monitoring and control measures in place
- has an approach that is consistent, and that performance is assured through audit and review
- assigns responsibility and personal accountability for risk management through all levels of management and staff, and individual performance is regularly measured
- fosters a culture of risk awareness and personal accountability to proactively disclose and address risk at all levels
- complies with applicable laws, regulations, Government directives and professional governance standards in the management of our material business risks.

3.2 Policy interpretation: What this means for you

Risk is an intrinsic aspect of the Commission's business environment. Risk can have negative (threat), or positive consequences (reward). Risk management is about managing both threat and reward. Innovation should be treated as a risk taken for a potential reward

Good risk management will not only look at the negative consequences of not being prepared for something which might happen (traditional risk management) but also the rewards to be gained by actively taking risks. By managing negative consequence risk diligently, and sensibly taking on the high reward risks, all staff can confidently say that they are doing everything possible to not only protect, but enhance our business.

The effectiveness of managing these risks, however, is mostly a reflection of our culture, values, and behaviours; and much less about adherence to process. Managing our risk exposure should be integrated into everyday activities. Being risk aware, understanding risk appetite and managing risk is not an add-on process, but a way of working, behaving and thinking about hazards and opportunities.

Staff are encouraged to adopt a pragmatic approach in implementing this policy, appropriate to the scale of the Commission activity in which it is applied.

Risk management accountabilities are individual and personal, not collective.

3.3 Risk management accountabilities

This policy requires commitment of all staff, and establishes the basis for assignment of accountabilities for oversight, implementation and operation of the risk management framework..

3.3.1 Commissioner

The Commissioner is ultimately accountable to Government for the effective management of material business risk, and is accountable for:

- approving the risk management policy
- approving the risk tolerance thresholds
- signing the annual attestation of compliance with core requirements (including risk framework, and management) in accordance with TPP 15-03
- providing direction and making decisions or escalating to Government, as required, for the management of risks graded as **HIGH**
- providing oversight and direction, as required, to the Executive Director, to ensure the effective implementation of the risk management and the risk management framework
- ensuring that adequate resources, including budget, are made available and are sufficient for managing the risk
- ensuring that an ARC is established to oversee and monitor governance, risk and control issues affecting the operations of the Commission
- approving the charter for the ARC, and monitoring and evaluating its performance.

3.3.2 The Commission

The Commissioner and the Assistant Commissioner, acting together in committee, constitute the 'Commission'. The corporate governance of risk and risk oversight is the responsibility of the Commission. The Commission is accountable for:

- establishing the risk appetite and agreeing on the risk tolerance thresholds
- reviewing the risk tolerance thresholds at least annually, or more frequently as circumstances dictate from time to time
- reviewing the risk profile, including material business risks at least quarterly, or by exception as required for risks graded as HIGH
- reviewing and satisfying itself with the effectiveness of the implementation and management of the risk management framework by the Executive Director, and the Commission management and staff, at least annually.

3.3.3 Shared Audit and Risk Committee

The Commission participates in the Department of Premier and Cabinet's Shared Audit and Risk Committee (ARC). The ARC is an integral component of the Commission's corporate governance arrangements. It has the specific objective of providing independent assistance to the Commissioner by overseeing and monitoring the Commission's governance, risk and control frameworks, and its external accountability requirements.

With respect to the Commission's risk management, the ARC is accountable for the following, and as otherwise set out in the ARC charter:

- reviewing whether management has in place a current and appropriate ERM process, and associated procedures for effective identification and management of financial and business risks, including fraud and corruption
- reviewing whether a sound and effective approach has been followed in developing strategic risk management plans for major projects and undertakings
- reviewing the impact of the risk management process on its control environment and insurance arrangements
- reviewing whether a sound and effective approach has been followed in establishing the business continuity arrangements, including whether disaster recovery plans have been tested periodically
- reviewing the fraud control plan and satisfy itself that appropriate processes and systems are in place to capture and effectively investigate fraud related information.

3.3.4 Executive Director

The Executive Director is directly accountable to the Commissioner for the following:

- developing and implementing the risk management framework
- periodically reporting on the effectiveness of the risk management framework, at least annually
- providing periodic reports, summarising the risk profile, material business risks and their management, to the Commissioner, at least quarterly and otherwise by exception for **HIGH** risks
- reviewing and effectively managing the material business risks
- assigning risk management accountabilities to team members, and providing appropriate resources to enable adequate risk management, including staff training where appropriate
- leading and fostering a culture of risk awareness, and personal accountability at all levels to proactively identify, disclose and manage risk
- issuing policies, procedures and other directives, as required from time to time, to ensure compliance with the risk management framework.

3.3.5 Director Corporate Services

The Director Corporate Services is administratively accountable to the Executive Director for:

- implementing and regularly reviewing, the approved risk management framework appropriate to the scale of the organisation and business operations
- undertaking the development of appropriate risk management procedures and assurance processes, fully integrated with 'business as usual' operations, management and administration
- conducting periodic risk reviews with management and staff, leading the identification, disclosure and analysis of risks, and maintaining the Risk Register

- assigning accountabilities to management and staff for risk controls and risk management
- preparing periodic risk reports for management, including escalation reporting of material business risks, at least quarterly, and otherwise as required to the Executive Director and the ARC
- monitoring compliance, and supporting continuous improvement of the risk management framework, and operational processes
- for the ARC, undertaking the role of internal audit officer, providing secretariat functions, supporting the ARC operations and administering and ensuring access to staff and information, as required or directed
- preparing and delivering risk management induction and other ongoing training, as required, for management and staff to ensure they are adequately prepared for their risk management responsibilities.

3.3.6 Chief Audit Executive

The Commission's 'Chief Audit Executive'[1], reports functionally to the ARC for strategic direction and accountability for the internal audit function – a key risk management control measure for the Commission. To ensure separation of duties, as defined by the Treasury guidelines, this role is performed by the Principal Risk and Audit Officer, Department Premier and Cabinet, under a principle-led agency agreement.

The reporting accountabilities of the Chief Audit Executive are illustrated in **Figure 2**.

[1] In accordance with TPP 15-03 Internal Audit and Risk management Policy for the NSW Public Sector

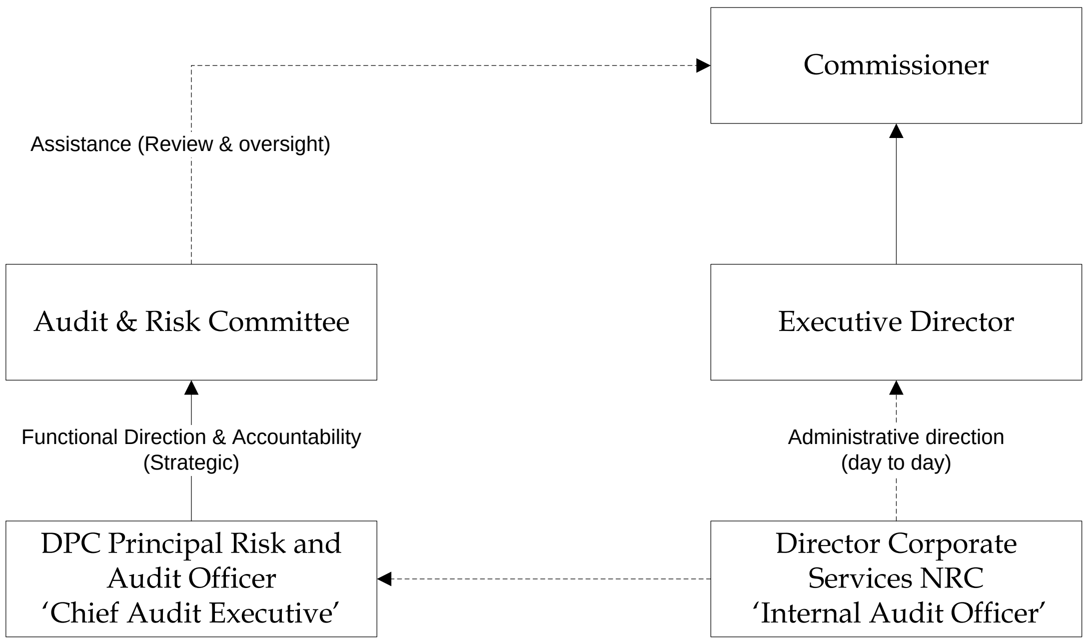

Figure 2: Chief Audit Executive reporting accountabilities

3.3.7 Staff, consultants and contractors

All staff are accountable for:

- identifying and managing risks as they pertain to their decision making. Refer to **Attachment 2** (Risk tolerance threshold matrix) for guide to risk ownership
- reporting to their manager any real or perceived risks that may significantly or materially affect the operational performance or reputation of the Commission, or that may leave the organisation exposed to legal or regulatory action. This includes any real or perceived risks to the health, safety and working environment of themselves, colleagues, customers or the general public; and any potential loss or damage to our assets and/or legal liabilities to third parties
- ensuring compliance with standards and requirements are fully and clearly communicated to all consultant and contract staff, and other stakeholders with whom the Commission does business, either internally or externally.

4 What is the risk management process?

Risk management within the Commission requires a disciplined approach and consistent process. The full risk management process[2] [3] has seven primary elements. **Figure 3** sets out the process.

[2] AS/NZS ISO 31000:2009; Risk management – Principles and Guidelines
[3] TPP 15-03 Internal Audit and Risk management Policy for the NSW Public Sector

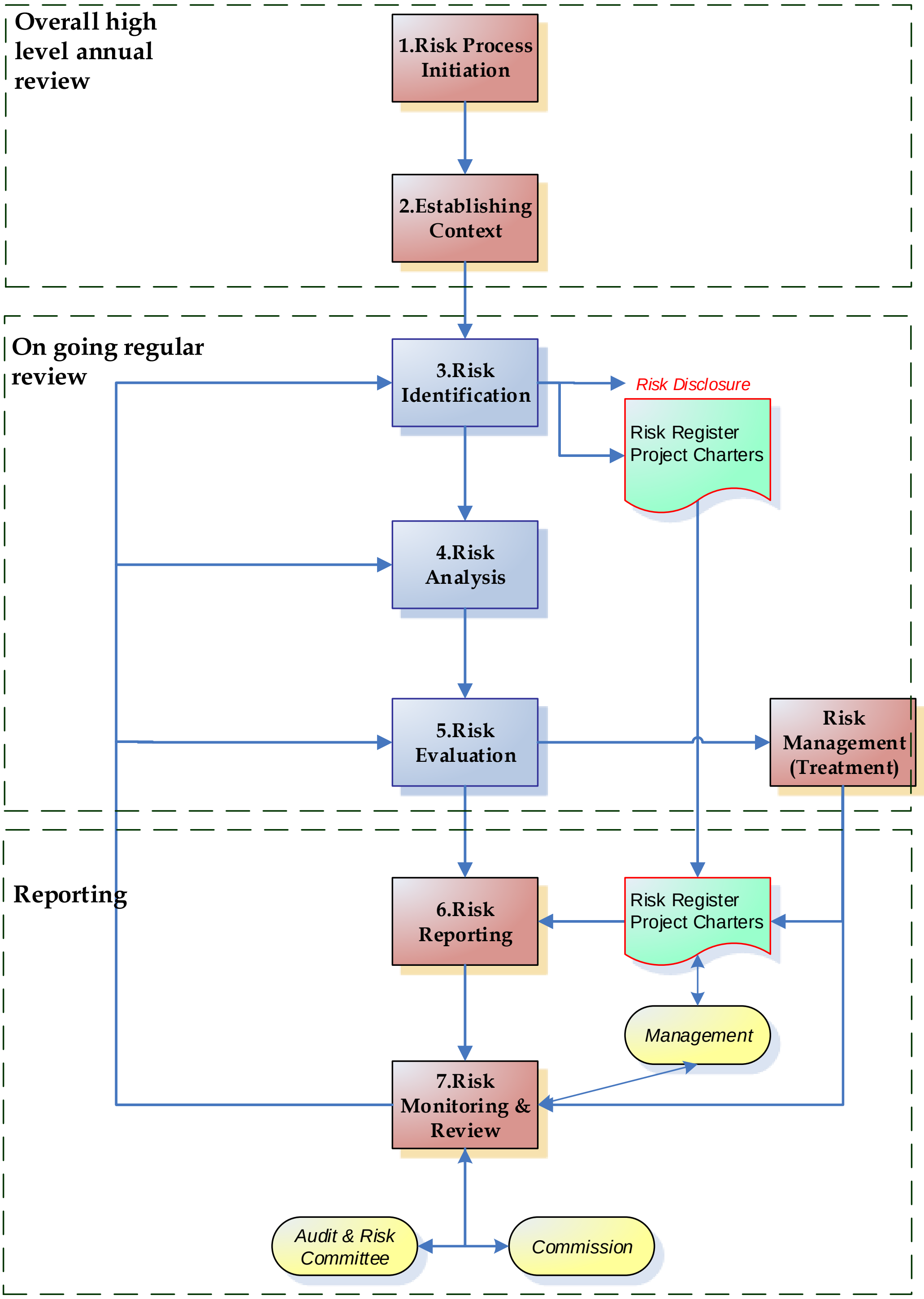

Figure 3: Risk management process

4.1 Risk process initiation and context

After creation of the framework, the risk process initiation and context form the strategic basis for the creation of the Commission's policy and framework. It is reviewed annually by the management team and is provided to the ARC for review and comment, and the Commissioner for approval.

4.2 Risk identification

Risk identification will occur as a result of one of the following:

- a formal general business risk workshop which should be undertaken at least annually
- a prescribed major activity or project related exercise which should be undertaken for every major project or event
- ad hoc risk discovery and exposure in the ordinary course of business.

Risk identification will typically be undertaken by the Director, Programs as a formalised element of project start up and planning phase, and will be recorded in the project charter for regular review and consideration during the term of the project.

The following checklist aims to help all staff in guiding and identifying risks in these phases:

- expose and identify all knowable risks
- separate risks, events or states from cause and effects
- identify possibility of risk aggregation
- manages bias
- identify risk owner.

Risk management is aligned with the project management system for implementation as follows:

Table 1: Integration of risk management into project management

Project management system	Aligned risk management process steps
Project initiation	Risk process initiation
Project strategy and scoping	Risk identification (ongoing)
Project start-up and planning	Risk analysis
	Risk evaluation
Project delivery	Risk management and treatment
	Risk reporting
	Risk monitoring and review (ongoing)
Project completion	
Project follow-up	

Risk identification in these project stages is the trigger for documenting and recording project risks in the project charter risk table and for risks being escalated to the Risk Register.

Risk identification leads to classification of the risk category, which will be confirmed during the risk assessment process.

The rationale for classifying risks is to provide a basis for their identification and control which are two essential parts of the risk management process.

Risk classification groups individual risks, having reasonably similar consequences, according to their estimated cost or likely impact, likelihood of occurrence, or counter measures required.

The risk classification structure is set out in **Section 4.8**.

4.3 Risk analysis

Risk analysis involves consideration of the causes and sources of risks, their positive and negative consequences, and the likelihood those consequences will occur. Factors that affect consequences and the interdependencies between risks should be identified. Analysis can be qualitative or quantitative or a combination of both, and the complexity of the analysis should be tailored to reflect the scale of the risk and activity.

Where appropriate, given the scale of the project or event, sensitivity of the risk to pre-conditions and assumptions should also be considered.

4.4 Risk evaluation

The purpose of risk evaluation is to assist in decision making, about which risks need treatment, and the priority for treatment implementation. The treatment decision will require synthesis of the analysis, to understand the likelihood and nature of the consequence. Consequences can either be:

- **economic** and can therefore be scaled: they affect budget, efficiency, productivity, staff (and stakeholder) utilisation or schedule
- **non-economic** and not scalable: they effect WH&S, compliance, community, or reputation for example.

Risk evaluation leads to identifying the risk materiality and relativity to the risk tolerance threshold.

4.5 Risk management and treatment

Risk treatment involves a cyclical process of:

- assessing risk treatment options
- deciding whether residual risk levels are tolerable
- assessing the effectiveness of the treatment.

Risk treatment action or decisions, often referred to as risk mitigation, can include:

- avoiding the risk by decision not to start, or to discontinue the activity giving rise to the risk
- taking or increasing risk inherent activity to pursue an opportunity
- removing the risk source
- reducing the risk likelihood
- changing the consequences
- sharing the risk with a party with the best capacity to manage the risk, including through contract and insurance

- retaining (and accepting) the risk through informed decision.

The treatment options are not mutually exclusive or appropriate in all circumstances. Control measures undertaken to modify a risk source, likelihood or consequence can include implementing (or applying existing) the Commission policies, processes, devices, or work practices.

Following treatment action, management and staff must be alert to the residual risk remaining after treatment. The revised risk profile (classification, likelihood and consequence) must be recorded in the Risk Register.

4.6 Risk reporting

Risk reporting does not obviate continuous risk disclosure, which should happen on discovery to management by any person becoming aware of such risk. Management must ensure that any disclosed risk is recorded in the Risk Register, and assessed, classified and appropriately treated.

The Risk Register should identify the:

- risk
- control and mitigation strategies to be applied
- level of residual risk.

Management report to the Commission must be at least six monthly, and quarterly to the ARC, or by exception as required.

4.6.1 Risk monitoring and review

Risk monitoring and review shall be undertaken, on both a programmed and ad hoc basis, as follows:

- enterprise risk workshop conducted annually by the Director Corporate Services with executive and senior management
- periodic review of the Risk Register or project risk registers conducted at least quarterly by the Director Corporate Services or Director respectively, or otherwise by exception as required
- review of Risk Register six monthly by the Commissioner or as required
- review of Risk Policy and Framework by the Commission at least annually
- review of Risk Policy and Framework and Risk Register by the ARC at least annually
- quarterly report to the ARC of extreme residual risks.

4.7 What is risk materiality?

The materiality of business risks relates to their potential to affect the deliverables, commitments, integrity and/or reputation of the organisation.

They may be defined via the quantitative or qualitative definitions that are relevant to the organisation and may include a broad range of risk types. Business risks include, but are not limited to, operational, financial, compliance, strategic, contractual, reputation, service quality, human resource, regulatory, industry and market related risks.

The materiality of any given risk is determined by reference to a threshold risk rating. The threshold risk rating is determined via assessment of the stated risk against the risk assessment matrix. This assessment involves an objective measure of the likelihood of the risk event or condition arising, and the consequences of the given risk should it arise.

Risks assessed at or above the acceptance threshold level are considered to be material risks.

The Commission will set and adjust risk materiality thresholds from time to time as the business, government, community, stakeholder and internal environment dictates. But these threshold measures must be reviewed by the Commission at least annually.

For material business risks, the required actions must include an understanding of:

- the effectiveness of the control and mitigation strategies to be applied
- the level of residual risk
- accountabilities for risk control actions
- accountabilities for risk control reporting and oversight.

4.8 What are the risk categories?

The categorisation of risk is a key element in enabling the identification, disclosure and analysis of risk. Risk classification is intended simply to group individual risks having reasonably similar expectations of loss according to their estimated cost or likely impact, likelihood of occurrence, or countermeasures required.

Risk categorisation and classification is therefore typically related to the sources or nature of the perils or hazards of risk exposure relevant to the nature of organisational business or its environment.

The following high level categories are therefore utilised to classify risk within the Commission:

- work, health and safety
- financial
- people and culture
- compliance
- service delivery
- business systems and operations, including Information Security Management Systems (ISMS) risks
- reputation.

These categories may be further subdivided or added to for specific risk analysis activities, such as for developing a major project risk management plan.

4.9 Analysis of risks

The following risk rating tables and matrices should be used to determine the severity of the identified risks. The tables and matrices are to be used in the following sequence:

- consequence of risk occurring
- likelihood of risk occurring
- assessment of the level of risk (i.e. combination of consequence and likelihood)

4.9.1 Consequence of risk occurring

Table 2 shows consequences of an identified risk.

Table 2: Risk consequence

Classification	Consequence
Extreme	Survival of the organisation is threatened
Major	Would produce a threat to the survival or effective performance of the organisation.
Moderate	Functions of the organisation could be subject to significant review or changes to operations.
Minor	A threat to the efficiency or effectiveness of some aspect of operations, but at a level which can be dealt with internally.
Insignificant	The consequences can be dealt with by routine operations.

4.9.2 Likelihood of risk occurring

Table 3 shows how to estimate the likelihood of an identified risk occurring.

Table 3: Risk likelihood

Likelihood description	Summary rating
Event almost certain to occur	Almost Certain
Event is likely to occur	Likely
Event may occur	Moderate
Event not likely to occur	Unlikely
Event rarely occurs	Rare

4.9.3 Risk classification rating

Table 4 shows a conversion matrix for the determination of the risk severity. Its purpose is to provide a uniform guide for management and staff to determine which risks are the highest priorities from the perspective of the timeliness of the corrective action required.

Table 4: Risk assessment matrix

	Consequences				
Likelihood	**Insignificant**	**Minor**	**Moderate**	**Major**	**Extreme**
Almost Certain	Moderate	Significant	Significant	High	High
Likely	Low	Moderate	Significant	High	High
Moderate	Low	Moderate	Significant	Significant	Significant
Unlikely	Low	Low	Moderate	Moderate	Significant
Rare	Low	Low	Low	Low	Moderate

Table 5 provides an explanation of the priority ratings used in the above guide.

Table 5: Risk classification rating

Legend	Explanation
High	Impact cannot be mitigated or controlled internally. Significant effect requiring immediate Commission directed and managed controls, and external agency or emergency service assistance
Significant	Impact requires additional/external resources to control. Executive Director directly undertakes or assigns senior officer responsibility to implement controls.
Moderate	Impact can be controlled with existing organisational resources. Management assigns responsibility for controls.
Low	Impact unlikely to require resources to control. Little or no effect on business. Managed by routine procedures.

4.10 What is the Risk Register?

Risk Register is used to identify the potential enterprise-wide risk categories and the controls in place to mitigate these risks. **Attachment 1** (Risk Register) details the nature of risk and the controls Commission has in place.

4.11 What is the risk tolerance threshold matrix?

This matrix establishes benchmarks for category consequence levels. **Attachment 2** (Risk tolerance threshold matrix) details the consequences and likely owners for different risk categories, identified by the Commission.

4.12 What is the risk dashboard?

The risk dashboard is part of the regular risk assessment conducted, and compliments the Risk Register by providing an overview of risk by category. It also includes raw and residual risk and trending of the risk. This provides users with a snapshot of all risks, allowing for easy identification and investigation, where necessary.

5 Document control

Date approved	March 2018
Review period	Annual
Next revision	March 2019
Responsible Officer	Director Corporate Services
Approving Officer	Commissioner
Changes made during the last revision	Edited text and adopted risk rankings to meet the DPC framework and the Audit Office Lighthouse model

Attachment 1: Risk Register example

See TRIM Document Number D12/0756 – Risk Register for current register

No	Nature of risk	Risk owner	Raw risk	Current control	Residual risk
1	**Compliance – Commission's risk appetite Low**				
1.1	Current policies and procedures within the Commission team environment are not complied with	Commission	L = Moderate C = Major	▪ Culture of compliance driven by the Executive team and Code of Conduct ▪ Internal audits on operational activities and on internal audit process ▪ ARC reviews ▪ Regular management, supervision and team communication in relation to policies and procedures ▪ Financial sign offs checked by external parties against delegated authorities ▪ Staff induction and training including the Commissioner ▪ Business plan (reviewed by the Commission every six months), operating strategy, and governance policy ▪ Regular review of policies and procedures as per the tracking register ▪ Regular briefings at team meetings ▪ Regular liaison with NSW and AG Ministers and Department Heads	L = Unlikely C = Minor

Attachment 2: Risk tolerance threshold matrix

		Consequence				
		Insignificant 1	Minor 2	Moderate 3	Major 4	Extreme 5
Risk categories	**Compliance**	Inadequate attention to legislation, contract, policy, or professional performance or standards resulting in inefficiencies.	Contract, policy, or professional breach leading to complaint.	Statutory, contract, policy, or professional breach leading to penalties or dispute with supplier, contractor or consultant.	Statutory, contract, policy, or professional breach, or systemic fault leading to escalated dispute, penalties, or legal sanctions. Key supplier, contractor or consultant termination due to unresolved breach of contract terms and conditions, or failure to deliver. Commission litigating contractual dispute, or defending a statutory compliance breach	Criminal legal sanctions and/or high cost litigation arising from statutory non-compliance or project failure. Commission (body corporate) suffers legal penalty or sanction.
	Risk owner	All Staff,	All Staff, Director, Programs, DCS	Director, Programs, DCS	Executive Director and Commissioner	Executive Director and Commissioner
	Financial	Variation of Commission budget of less than $20,000 Individual project budget variation of less than 5 per cent	Variation of Commission budget of between $20,000 to $50,000 Individual project budget variation of less than 10 per cent	Variation of Commission budget of between $ 50,000 and $200,000 Individual project budget variation of less than 20 per cent	Variation of Commission budget of between $200,000 and $500,000. Individual project budget variation of $200,000 and $500,000	Variation of Commission budget of greater than $500,000 Individual project budget variation of greater than $500,000
	Risk owner	Director, Programs, DCS	DCS, Director, Programs and Executive Director	Director, Programs and Executive Director	Executive Director and Commissioner	Executive Director and Commissioner

		Consequence				
		Insignificant 1	**Minor 2**	**Moderate 3**	**Major 4**	**Extreme 5**
	People & Culture	Staff losses at or below benchmark standards. All staff generally meeting performance and development expectations.	Staff losses at or marginally above benchmark standards. Most staff generally meeting performance agreement Providing non-conventional training options	Staff losses greater than benchmark standards; delays in recruiting staff. One or more key staff performing at or near minimum performance expectations. (Commission has a low risk tolerance/appetite here)	Loss of key staff; and difficulty attracting staff. Key staff not meeting performance and development expectations; require performance management.	Significant loss of staff; and inability to attract staff. Many key staff failing to meet minimum performance and development expectations; require managing out of business.
	Risk owner	All Staff	Director, Programs, DCS	Director, Programs, DCS	Executive Director and Commissioner	Executive Director and Commissioner
	Work Health and Safety	One or more incidents with no injuries, and no time loss; but no 'near hits or near loss' incidents. Staff sick leave below benchmark levels.	A single 'near hit/near loss' incident which would have incurred a serious injury or time loss. One or more minor first aid or medical treatment injuries. Staff sick leave at benchmark levels.	Multiple 'near hit/near loss incidents'; One or more serious medical treatment and lost time injury incidents. Higher than average staff numbers with sick leave. Any work place related physical or psychological health impact or deterioration causing lost time and/or reduced work capacity to one or more staff.	Serious injuries/permanent incapacity to one or more staff. Community pandemic illness affecting high staff numbers, sporadic office and/or project closures. Serious workplace related physical or psychological health impact or deterioration causing long term reduced work capacity to one or more staff.	One or more fatalities, and/or multiple serious injuries. Community epidemic illness affecting significant staff numbers, who are unable to work, team, function and/or project shutdowns. Life threatening workplace related physical or psychological health impact, or deterioration causing total permanent incapacity to one or more staff
	Risk owner	All Staff	Director, Programs, DCS	Director, Programs, DCS	Executive Director and Commissioner	Executive Director and Commissioner

		Consequence				
		Insignificant 1	**Minor 2**	**Moderate 3**	**Major 4**	**Extreme 5**
	Service Delivery	Minor deliverable rework at own or client request, without cost or schedule impact	Rework on deliverable with cost and or schedule impact; may include formal complaint or redress from client	Work backlog less than six months with few qualified opportunities, and few additional prospects for future engagement. Insufficient resources available to meet one or more project commitments, or achieve one or more business objectives. Substantial re-work on deliverable required with significant cost and schedule impact. Not achieving project or functional targets.	Work backlog less than three months, with few qualified prospects, and few or no prospects for future engagement. Insufficient resources to meet many commitments or business objectives Project termination and/or loss of client confidence due to poor delivery. Commission not achieving one or more critical strategic objectives.	Work backlog less than one month with no qualified pipeline opportunities for work engagement. Commission substantially unable to meet its commitments and obligations. Commission's key strategic service suspended or terminated by Government. Commission fails to achieve all or most strategic objectives.
	Risk owner	All Staff	Director, Programs, DCS	Director, Programs, Executive Director	Executive Director and Commissioner	Executive Director and Commissioner

		Consequence				
		Insignificant 1	**Minor 2**	**Moderate 3**	**Major 4**	**Extreme 5**
	Business Operations	Single isolated non-core system temporary failure or recoverable data loss at the desktop level. Functionality and service restored through routine actions in less than 2 hours. Locally isolated temporary network and/or system performance degradation Help Desk and Technical Service incidents below benchmark and within SLA thresholds.	Business continuity disrupted due to failure of one core system and/or non-critical data loss. System disaster recovery less than 4 hours. Intermittent network and/or system performance degradation, one or more minor desktop temporary disruptions. Help Desk and Technical Service incident reports at benchmark and SLA thresholds.	Business continuity disrupted due to failure of one or more management information systems (such as TRIM). System disaster recovery exceeds 4 hours. Intermittent or single incident network wide and/or system performance degradation incident, impacting business as usual Help Desk and Technical Service incident reports and response dissatisfaction exceed benchmark and SLA thresholds.	Business continuity disrupted organisationally wide due to one or more core system failures and/or critical data loss. System disaster recovery exceeds 48 hours. Frequent and widely distributed network and/or disaster performance degradation, impacting total organisation business as usual. Help Desk and Technical Service incident reports and response dissatisfaction significantly exceed benchmark and SLA thresholds; additional resources re-assigned internally and/or external assistance required.	Unrecoverable core system failure and/or critical data loss. System disaster recovery exceeds 5 days. Beyond capability and/or capacity of service delivery agency staff to resolve. Substantial external emergency assistance required.
	Risk owner	All Staff	Director Corporate Services	Director Corporate Services	Director Corporate Services, Executive Director	Executive Director and Commissioner

		Consequence				
		Insignificant 1	Minor 2	Moderate 3	Major 4	Extreme 5
	Reputation	Individual staff member capability questioned (internal)	Stakeholders or client requires 'hard work' to engage with Commission advice. Individual employee, consultant or contractor probity, competence, or professionalism questioned by or compromised with client. Minor stakeholder disputes Commission audit findings or advice, may enrol other stakeholder agencies/departments in support.	Thought leadership advice makes recipients uncomfortable. Commission project team or organisational credibility or capability criticised by client, key stakeholder, professional standards, or regulatory authority.	Government questions the credibility of key elements of the advice, methodology or evidence in a major report, and may reject one or more of those key elements in the report. Publicly disclosed or exposed professional performance issues, in one or more local regional or NSW state media services. Commission's professional integrity called into question by DPC, State parliament, ICAC or police. Commission perceived as lacking independence, scientific credibility or relevance with Government.	Government or key stakeholder (i.e. LLS Chairs) substantially reject and openly question the credibility of advice, methodology, evidence or science in one or more major reports. Major local, state, national and/or international negative media coverage; leaving the Commission negatively impacted on a state-wide scale. Commission staff convicted of fraud, corruption, or other wrongdoing.
	Risk owner	All Staff	Director, Programs, Executive Director	Director, Programs, Executive Director	Executive Director and Commissioner	Executive Director and Commissioner

The Commission and staff are responsible for identifying and managing risks as they pertain to their decision-making.