Enterprise Risk Management Framework

1. Purpose

Risk is defined as the effect of uncertainty on objectives. This Framework is intended to provide the NSW Department of Industry ('the Department'), and its Divisions and Branches, with a description of the expectations and structure in which the consistent application of Enterprise Risk Management (ERM) principles are to be applied.

2. Scope

This framework and all associated procedures applies to all Departmental workers including employees, contractors, relevant consultants engaged in a management capacity, volunteers and any other person working within the Department with staff responsibilities. The Department has designed its framework to be consistent with the requirements of the following:

- Australian / New Zealand Standard for Risk Management, AS/NZS ISO 31000:2009
- NSW Treasury *Internal Audit and Risk Management Policy for the NSW Public Sector*, TPP 15-03

3. Mandate and commitment

The Executive are committed to good corporate governance and creating a positive organisational culture that promotes risk management acceptance, communication and management of appropriate risk at all levels of the Department. Within the Department, risk is guided by the following principles:

- All staff are responsible for the proactive identification, escalation and management of risk.
- All risks are considered relative to the Department's strategic priorities.
- ERM follows the strategic planning framework, cascaded from the top-down, and systematically managed bottom-up through all levels of the Department.
- The level of response to risk is proportionate to its likelihood and consequence.
- The level of response is proportionate to the risk appetite
- The Corporate Strategy (CS) branch is responsible for the framework of policy, tools, training and documentation. The CS branch works with risk functions within the Department to ensure consistent application of the framework across the Department.

4. Risk management objectives

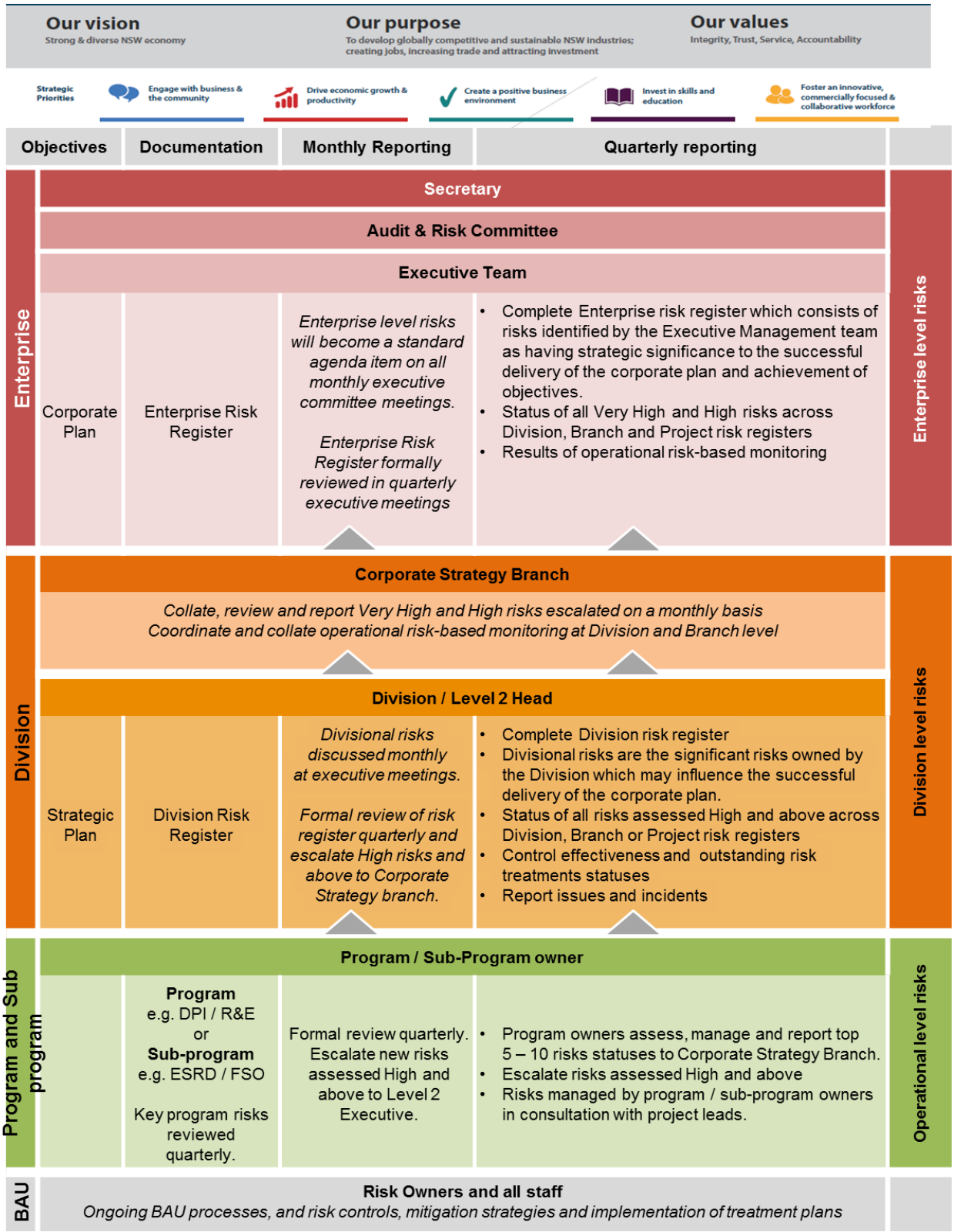
The Department requires a strong risk culture to enable it to deliver on its vision and purpose. The Department's tolerance for risk as it relates to specific functions undertaken by the Department is outlined in its risk appetite statement. This culture and consistent approach to risk is integrated into the Department's core business and embedded within planning processes, decision making structures and operational procedures at every level of the Department.

5. Risk management strategy

Effective risk management enables the Department to meet its challenges in delivering on its Corporate Plan and objectives at each level. The Department does so by operating within a hybrid structure of devolved responsibility within a three level structure for risk management. Although the Department Secretary has the ultimate responsibility and accountability, risk management is everyone's responsibility. This responsibility is a structured, consistent and continuous process used at the:

- Enterprise level (Key risks identified by the executive as being of strategic significance)
- Divisional level (Significant risks owned by each division which may impact on strategic objectives)
- Operational level (Risks that exist within programs or subprograms of work):

The following diagram describes the Department's strategy for managing risk, reporting expectations, and the content at each level to ensure appropriate visibility for risks throughout the Department.



Enterprise Risk Management Structure

Risk priorities are cascaded down from the Enterprise level to the Division and operational levels in the same way as the Corporate Plan cascades down to Division and program / sub-program plans. The risk resources at each level of the Department are responsible for the aggregation of relevant information affecting the likelihood and impact of risks for the Department, to make an accurate assessment of residual risk.

Enterprise level

The CS branch has been delegated the responsibility for operationalising this ERM Framework across the Department, including ownership of all risk policies, tools and procedure documents. The CS branch oversees all risk reporting to the Audit and Risk Committee (ARC) and the Executive. The CS Branch is supported by risk functions in each Division and other work units that report to the Secretary.

The Enterprise Risk Register captures strategic risks to achieving the Corporate Plan, and is a reflection of the top-down and bottom-up risk priorities of the Department.

This register is owned by the Department Executive responsible for risk, and maintained by the CS Branch. This register must represent an aggregation of the ERM information for the enterprise.

Division level

Level 2 Executives reporting to the Secretary have responsibility for undertaking a risk function within their Division or work area. In consultation with the CS Branch (and the Executive responsible for risk management) the Division or work area must maintain a risk capability at a level that is adequate to support the nature, extent and complexity of the operations undertaken.

The Division/work area-focused risk functions report on risks based on the Division's Strategic Plan (or Corporate Plan, in the case of work areas), and mapped to the five strategic priorities of the Department. The function and register are responsible to the respective Level 2 head, and have dotted line reporting to the CS Branch. The Level 2 head is accountable for the Division's/work areas risk register, and the Division/work area risk function has responsibility for maintenance of the register.

Operational level

Operational risk is managed at the Program and Sub-program level by Branch Directors. To avoid unnecessary reporting, the Department does not mandate branch risk registers, but focuses on managing risk operationally through its programs and sub-programs, which form the foundation of its strategic planning and reporting framework.

The program or subprogram owner maintains a program or project risk register associated with delivery. It is the responsibility of the program/subprogram owner to facilitate regular discussions around risk and to escalate any high or very high risks to the Level 2 Head.

The Department has established specific policies, procedures and guidelines to ensure the effective management of risk in many of these common operational areas, which are supported by steering committees in some instances. The areas include, but not limited to:

- Financial management
- Work Health Safety
- Legal / Regulatory
- Business continuity, Emergency management, and disaster recovery planning
- Change management
- Fraud and Corruption Prevention
- Emergency management
- Program management and delivery
- Procurement
- Stakeholder management
- Strategic delivery
- Governance
- People management
- Systems management
- Operating environment

6. Risk management roles and responsibilities

The Department's risk management and reporting structure consists of three distinct management levels, with roles and responsibilities within the risk function are described below.

Role	Description
Secretary	The Secretary is accountable for ensuring the effective implementation of the ERM framework within NSW Department of Industry. This includes: ▪ Approving the ERM framework, including policy, procedures and plan. ▪ Determining the Department's risk appetite. ▪ Ensuring the ERM framework is implemented and reviewed regularly. ▪ Reviewing recommendations from the Audit and Risk Committee (ARC). ▪ Promoting a positive risk culture. ▪ Ensuring that managers, decision makers and all staff, are accountable for managing risk within their respective roles. ▪ Attesting compliance with the eight Core Requirements of TPP15-03 annually.
Executive Team e.g. Deputy Secretary, Director General DPI, relevant Direct report to the Secretary	Each member of the Executive Team supports the Secretary in the operationalisation of risk management for their area of responsibility by: ▪ Setting the mandate and commitment for risk management. ▪ Leading and aligning the Department's risk culture. ▪ Leading ERM framework implementation within their area of responsibility. ▪ Aligning Corporate and Division strategic priorities with risk management objectives. ▪ Ensuring legal and regulatory compliance. ▪ Ensuring adequate resources are allocated for the management of risk at the Enterprise and Division levels. ▪ Assigning risk ownership within their Division. ▪ Promoting and effecting visibility of their respective Divisional risks and their treatments at the Enterprise level and associated information flow. ▪ Reviewing and challenging risk assessments during review processes and escalating risks assessed High or above to Corporate Strategy (CS) Branch. ▪ Completing quarterly risk management attestation.
Corporate Strategy (CS) Branch	Corporate Strategy (CS) Branch is accountable for the ERM framework and works closely with the Executive Team, Division Executives, and Program / Sub-Program owners to: ▪ Coordinate establishment of accountability, authority and appropriate competence for managing risk, including implementing and maintaining the risk management process and ensuring adequacy, effectiveness and efficiency of controls. ▪ Coordinate the integration of risk management into Department processes, ensuring that risk management is part of, not separate from these processes. ▪ Coordinate internal communication and reporting mechanisms to support accountability and ownership of risk. ▪ Develop risk capability across the organisation and promoting best practice ▪ Review and ensure the ERM framework remains appropriate. ▪ Challenging the robustness of risk assessments, proposed risk treatments and related documentation within each Division or work area.
Program/ sub program owner	Program/ Sub program owners are responsible for the effective management of risks in their programs, including: ▪ Maintaining a register of key risks associated with the delivery of their program ▪ Facilitating risk discussions with risk owners that contribute to successful program/ sub program delivery. ▪ Reviewing, reporting and escalating risks assessed high or above to Division / Level 2 Head.
Risk Owner	Risk Owners are responsible for the day-to-day management of risk and ensuring relevant risk registers are updated and allocated treatments actioned.

Role	Description
All staff	All staff are responsible for the management of risk within their sphere of influence. This includes: ▪ Using a risk management approach in all decision making. ▪ Familiarisation with the risk management process and its application within their areas of responsibility. ▪ Participation in the identification, assessment, reporting and management of risk. ▪ Applying risk plans in their areas of responsibility by identifying, communicating and responding to expected or emerging risks.
Chief Audit Executive (CAE)	The role of the CAE is to set and fulfil an internal audit plan, ensuring the current risk profile is relative to the risk appetite of the Department and providing assurance to the Secretary and ARC over the following: ▪ The Department's financial and operational controls are operating in an efficient, effective and ethical manner. ▪ The effectiveness of the risk management framework including the design and operational effectiveness of internal controls. ▪ Risk exposures relating to the organisation's governance, operations, and information systems are correctly evaluated. ▪ Evaluate the effectiveness of, and contribute to the improvement in, risk management processes ▪ Assisting management to identify risks and develop risk treatments and monitoring strategies as part of the risk management framework. ▪ Advising relevant stakeholders (including CS branch) of internal and external audit findings which identify risk and control vulnerabilities.
Audit and Risk Committee (ARC)	The objective of the ARC is to provide independent advice to the Department by overseeing and monitoring its governance, risk and control framework, and its external accountability requirements. The responsibilities of the ARC include: ▪ Reviewing whether the Department has in place a current and appropriate ERM process. ▪ Reviewing whether a sound and effective approach has been followed to develop risk management plans for major projects and undertakings. ▪ Reviewing internal and external audit findings which identify possible risk and control weaknesses and monitoring management actions until completed. ▪ Review risk reports and provide advice to the Secretary. ▪ Reviewing other risk management arrangements as set out in the Committee's Charter and as specified in Treasury guidance.

Three Lines of Defence

The Department has adopted the "Three Lines of Defence model" to ensure there are clearly defined risk ownership responsibilities within functionally independent levels of advice, oversight and independent assurance. Each of these lines has a distinct role in the Department's governance and oversight.

First line of defence – Risk Owners

The first line of defence comprises management and all line employees who assume ownership of risks and their management. Management are responsible for day-to-day risk management decision-making involving risk identification, assessment, mitigation, monitoring and management. The first line of defence includes all staff, managers and directors involved in delivering and fulfilling the Department's functions and obligations.

Second line of defence – Advise, Review and Challenge

The second line of defence comprises the CS centralised risk management function and any other quality assurance or review committees that are functionally independent from the first line of defence.

Third line of defence - Independent Assurance

The third line of defence comprises the Department's Internal Audit function which is independent of front line staff and service delivery areas and the Department's Audit and Risk Committee, each of whom provides independent assurance to the Executive Team and ultimately the Secretary on the effectiveness of risk management throughout the Department.

7. Risk management process

The Department follows the guidance in AS/NZS ISO31000:2009 for risk management. To ensure consistency throughout the Department, all employees follow this same process for the identification and assessment of likelihood and consequence of uncertain adverse events at the Enterprise, Division, Branch / Program level and Sub-program / Project level.

Based on that assessment effort, controls and monitoring are applied, relative to the treatment of any adverse outcomes to achieve the target risk rating.

Stage 1: Establish the Context

At the commencement of a risk assessment process, establishing the context defines how the risk management process should be applied. It includes the following activities:

- Defining the objectives for risk management on the business activity or project.
- Any assumptions that underpin the scope of business operation or project, which need to be considered.
- Who will be involved, and their roles and responsibilities in relation to risk.
- Forum and frequency of risk review.
- How the results of risk assessment will guide risk treatment.
- How the team will meet the Department's risk management and reporting requirements.

The outcome of this stage is a plan that defines the scope and context of risk management activities and how it will apply.

Stage 2: Identify

This stage seeks to identify the risks that may prevent, degrade, delay or enhance the achievement of the Department's objectives, in the context that has been agreed in **Stage 1.**

Effective identification should be driven by the Department's Corporate Plan, and the history, experience, and internal and external information available about the relevant Enterprise, Division, Branch / Program or Sub-Program / Project objectives and operations.

Following identification, as a minimum, the below information must be recorded in the risk register (Attachment C):

- Risk description (try and describe as an event or something that could have a post event analysis performed if it were to occur)
- Potential causes
- For divisional risks, appropriate linkage to relevant enterprise risks
- Current controls in place to manage the risk
- What actions (risk treatments) are required to bring the risk severity within ALARP
- Key risk indicators
- An appropriate owner for the risk.

Stage 3: Analyse risks

Analysing the risks involves the following steps to determine the **current risk rating** and **target risk rating**. To ensure there is a consistent approach to risk assessment and management, consequence and likelihood descriptors have been developed that can be applied regardless of where the risk is identified within the Department (Attachment A).

Likelihood and consequence must be considered separately before using the Department's risk matrix to determine whether the risk is:

- Very High
- High
- Medium
- Low

For consequence, you should consider the risk against each of the consequence criteria in the matrix, and the category with the most severe consequence is used to determine the consequence level of the risk.

Current risk rating

Current risk is assessed through the consideration of the identified risk in the context of what is currently being done to manage the risk (i.e. the controls that are in place). This allows you to determine whether the risk is within the Department's risk appetite and whether additional treatments are required to mitigate the risk further. To determine the current risk rating, consider:

- The current likelihood of the risk is determined by considering the effect of any actions or controls currently in place and assessing the likelihood of the risk occurring against the descriptions from the assessment criteria (Attachment A, Table 1).
- Assuming the risk did occur, rate the most likely impact, score the impact against each of the six categories of consequence, taking into consideration the current operating environment and effect of any actions or controls currently in place (Attachment A, Table 2).
- Identify the risk rating, using the likelihood and greatest consequence measure against the risk matrix (Attachment B).

To ensure the quality of each risk assessment, all assessed risks should be challenged and subjected to review and approval by the relevant Division or Enterprise risk team. This review will ensure consistency of approach and limit the possibility of risk duplication.

Stage 4 & 5: Evaluate and treat risks

To address these risks, suitable treatment responses will take into consideration the consequences on strategic and service delivery, safety, financial, environmental and stakeholder and reputational considerations, and treatment actions will be documented in the relevant risk register.

Target risk rating

Once a risk has been analysed, the current severity rating must be considered to determine whether the risk rating is as low as reasonably practicable (ALARP) exposure for the Department. A risk that is assessed as not ALARP, a target risk rating in order to eliminate, manage or reduce the risk to an acceptable level must be determined.

To reduce a risk assessed as not ALARP to an acceptable level, additional controls or treatments will need to be implemented to reduce the expected likelihood or consequence of a risk, enabling the Department to reach the target risk rating.

Risk Treatments

To develop and approve risk treatments across the Department, the following delegations must be followed to ensure the appropriate treatment and coverage of risks. The treatment of each risk must also have a designated owner and due date, which must be captured in the risk register.

Very High	Only the Secretary of the Department can approve the acceptable management actions for a Very High current risk.
High	Division / Level 2 Head can approve the acceptable management actions for a High current risk.
Medium	The relevant Branch Director can approve the acceptable management actions for a Medium current risk.
Low	A Low risk can be managed through the routine operations of the Department under the oversight by the relevant Branch Manager, who is responsible for reasonable monitoring of change / variances in the likelihood and consequences.

Stage 6: Monitor and Review

Risk owners are required to perform regular monitoring of risks, control effectiveness, current risk ratings and action status for all risks to confirm impact of any changes in conditions / environment.

The CS Branch will meet regularly with Division risk resources to formally assess the risk ratings, and progress of management actions. This allows the Department to assess the effectiveness of the risk management process on an ongoing basis, as well as undertake a thorough review of the Department's risk registers, in particular, assist in identifying and monitoring risks applying to more than one division. The identified risks and the effectiveness of risk treatments will be reviewed to reflect changing circumstances and priorities. Specifically, CS Branch will review Very High and High risks which have been escalated on a monthly basis at the Division, Program and sub-program level, as well undertake operational risk-based monitoring.

Where a review finds that a risk has increased in rating, it must be escalated and managed in accordance with the table above.

Stage 7: Communicate and consult

The Secretary must provide to the Treasurer, in the annual report and in the Attestation Statement, a confirmation that risk is managed effectively. Communication and Consultation, including through risk reporting is required throughout the risk process to ensure there is clear understanding of the status of risks, controls and treatments and the reasons behind decisions and actions.

8. Continual improvement

The Department is committed to continuous improvement of the ERM framework. The CS Branch will coordinate the continual improvement of the Framework by recommending improvements to decision makers (including the Department Executive) based on the aggregate of the information reported.

To ensure the ERM framework continues to reflect the current needs and commitment of the Department, the CS Branch will:

- Conduct an annual review and update of this document.
- Annual assessment of the quality of business processes and controls.
- Ongoing training and development, including communication of lessons learnt and continuous risk management learning to all staff.
- Measure the Department's performance with regard to risk management and other key governance processes.

Definitions

- **Enterprise Risk Management (ERM)**: is an ongoing process, affected by people at every level of the Department, designed to identify potential events that may affect the achievement of the Corporate objectives.

- **Objectives**: are specific, realistic and measurable goals which enable the Department to deliver on its priorities within a given period of time as expressed in the Corporate Plan.
- **Risk**: the effect of uncertainty on objectives, noting that effect is a deviation from the expected and may be positive and/or negative.
- **Risk treatment**: is the process used to modify risk; including the elimination or strategy to reduce the likelihood and/or severity of the negative consequences. They could be specific actions, policies, procedures or additional controls that need to be developed.
- **Likelihood**: chance of something happening.
- **Impact**: the amount of loss or gain that is sustained from the consequence of a risk.
- **Consequence**: outcome of an event affecting objectives.
- **Current risk**: a subjective measure of the risk **after** action has been taken to manage it.
- **Risk register**: Part of the risk management plan that identifies risks, evaluates them and identifies current or future risk treatments and controls to modify the risk.
- **Controls**: measures that modify risk such as processes, policies, devices, practices or other actions that act to minimise negative risks or enhance positive opportunities
- **As low as reasonably practicable (ALARP)**: the risk rating that demonstrates that the cost involved in reducing the risk further would be disproportionate to the benefit gained.

Related attachments

- Attachment A – Risk Likelihood and Consequence descriptors
- Attachment B – Matrix for Risk Ratings

Related documents

- NSW Department of Industry Risk Appetite Statement
- NSW Department of Industry Risk Management - Help Card No.1 – A Guide to Developing a Risk Register

Superseded documents

These document replaces:

- I&I NSW Enterprise Risk Management procedures
- NSW Trade & Investment Enterprise Risk Management policy
- NSW Trade & Investment Enterprise Risk Management implementation procedure

Revision history

Version	Date issued	Notes	By
1.0	10/04/2012	New document following merger / creation of NSW Trade & Investment	**Manager, Corporate Governance**
2.0	11/05/2016	Revised draft for ARC consideration	**Manager, Corporate Governance**
3.0	27/05/2016	Updated following ARC review	**Manager, Corporate Governance**
4.0	24/06/2016	Updated following early consultation with Divisions	**Director, Corporate Strategy**
5.0	23/06/2016	Updated brief endorsed by EMC	**Director, Corporate Strategy**
6.0	23/06/2017	Updated *Related documents* section by adding Risk Management - Help Card No.1- A Guide to Developing a Risk Register. Document number amended from IND-I-207 to IND-P-207 due to policy library category change.	**Manager, Corporate Governance**

Review date

23/6/2018

Contact

Manager, Corporate Governance

Attachment A – Risk Likelihood and Consequence descriptors

Table 1: Likelihood of risk occurring

Likelihood				
		Qualitative	Probability	Frequency
5	Almost certain	Occurs often	95 - 100%	>10 times per year (Could occur on a daily / weekly basis)
4	Likely	Likely to occur	50 - 95%	2 - 10 times / year (Could occur on a monthly /quarterly basis)
3	Possible	Could occur, but more than likely it will not.	20 – 49%	Once every 1 –10 years
2	Unlikely	May occur only in unusual circumstances	1 - 19%	Once every 10 – 100 years
1	Rare	Would only occur under exceptional circumstances.	<1%	Once every 100 to 1,000 years

Level	Health & Safety	Environment & Heritage	Governance & Compliance	Industry & Customer Experience	Stakeholder Trust / Confidence	Service Delivery	Value & Benefits	Financial
5 Extreme	Health & Safety risks are to be assessed and managed in accordance with the Health and Safety Policy and related procedures.	**Irreversible** large-scale environmental impact with **loss of valued ecosystems**.	**Prosecution** leading to imprisonment of executive(s). Significant **prosecution / litigation**. **Loss of operating licence.**	Extensive shutdowns or extended disruptions with **economy-wide** and national effects. **Structural change** or **long-term** Industry impact.	**Outrage** — Material change in the public perception of the organisation. Confidence and trust are severely damaged. possibly irreparably. and full recovery both questionable and costly.	**Catastrophic** event with the clear potential to lead to the collapse of the organisation.	Failure to realise benefits of **enterprise-wide operations**: or publicly announced portion/ milestone significantly missed or final completion date significantly missed on critical path project.	>$50m **OR** >45% of Budget
4 Major		Long-term environmental impairment in neighbouring or valued ecosystems. **Extensive remediation required**.	**Substantial breach** resulting in prosecution. fines and/or litigation. Licence or accreditation **restricted or conditions** affecting ability to operate.	Short duration shutdowns or substantial disruptions affecting **multiple industries** with **state or sector-wide** cascading effects.	**Displeasure** — Extended negative state/national media coverage. Confidence and trust are damaged but recoverable at considerable cost. time and staff effort.	**Severe event** which requires **extensive** management effort but can be survived.	**Severe delays with initiative** which impacts **across divisions** and/or significant decrease in benefits realised: or publicly announced portion/milestone missed or final completion date missed on critical path project.	>$5M - ≤$50M **OR** 45% of Budget
3 Moderate		Impacts external ecosystem and **considerable remediation** is required.	**Breach resulting in enforcement action** and/or prohibition notices. Substantial fine and no disruption to services.	**Significant** disruptions affecting operations of **one industry sector or region** with state-wide effects on one or more other regions or sectors	**Concern** — Short-term negative state/national media coverage. Confidence and trust are diminished but are recoverable with time. staff effort and additional funding.	**Significant event** which can be absorbed. but **substantial** management effort is required.	**Significant delays with initiative** and/or **major decrease in benefits realised**: or publicly announced portion/milestone missed or final completion date missed with demonstrable mitigating external circumstances.	>$500k - ≤ $5M **OR** 25% of Budget
2 Minor		**Short-term** and/or well-contained environmental effects. **Minor remedial** actions probably required.	**Significant non-compliance**. Subject to comment and monitoring from applicable regulator. Small fine and no disruption to services.	**Serious** disruptions affecting operation of **one industry sector or region**.	**Disappointment** — Extended negative local/state media coverage. Confidence and trust dented but are quickly recoverable at modest cost within existing budget and resources.	**Minor event**. the impact of which can be absorbed but much **broader** management effort is required.	**Several delays** with the initiative and/or moderate decrease in benefits realised: or completion date missed for non- critical path project.	$50k - ≤ $500k **OR** 10% of Budget
1 Insignificant		**Change from normal** conditions within environmental regulatory limits and environmental effects are within site boundaries.	**Minor non-compliance** with legal and/or regulatory requirement or duty. Investigation and/or report to authority.	**Minor disruptions** affecting several industries or regions.	**Unease** — Series of negative articles in local/state media. Confidence remains with some minor loss of goodwill or trust. Recoverable with little effort or cost. Some continuing scrutiny/attention.	An event. the impact of which can be absorbed but **some additional** management effort is required.	**Minor delay** with the initiative and/or a minor decrease in the benefits realised: or minor delay on the project or another project. with no public implications.	≤ $50k **OR** 5 % Budget

Table 2: Qualitative descriptors of consequence or potential impacts

Attachment B – Matrix for Rating Risks

Consequence	Likelihood				
	E. Rare	D. Unlikely	C. Possible	B. Likely	A. Almost Certain
5. Extreme	Medium	High	High	Very High	Very High
4. Major	Low	Medium	High	High	Very High
3. Moderate	Low	Medium	Medium	High	High
2. Minor	Low	Low	Medium	Medium	Medium
1. Insignificant	Low	Low	Low	Low	Medium

General Risk Tolerance & Review Guide			
Risk Rating	**Basic Tolerance**	**Basic management, escalation and reporting**	**Review frequency**
Very High	Generally intolerable.	Must obtain seek Secretary approval for Risks and their Treatments at this level	Monthly
High	Undesirable	Must obtain Director General or Deputy Secretary approval for Risks and their Treatments at this level. Director General or Deputy Secretary to escalate to Secretary as appropriate	Quarterly
Medium	Tolerable	Business owner to review Risks and their Treatments at this level	6 Monthly
Low	Broadly acceptable	Business owner should review Risks and their Treatments at this level for effectiveness and reliability.	Annually