Risk Management Framework

Summary:

This procedure describes TransGrid's risk management framework and high-level process and provides the structure and tools that will facilitate the use of a consistent risk management process, whenever decisions are being made in TransGrid. TransGrid undertakes risk management processes to improve decision making by understanding the effect of uncertainty on achievement of business objectives.

Successful management of risk can:

- Improve organisational performance and increase organisational resilience
- Reduce foreseeable threats to a level that TransGrid is willing to accept
- Enable TransGrid to maximise opportunities that may present themselves.

Revision no: 7	Date: 13/5/2014
Business function: Manage Risk	Document type: Framework
Process owner: Corporate Audit and Risk Manager	
Author:	Meredith Sturman, Corporate Audit and Risk Manager
Reviewers:	Stuart Johnston, Corporate Environment Manager; Ken Carroll, Manager/Quality and Business Improvement; Ken McCall, Manager/Health and Safety; John Howland, Manager/Portfolio Management Office; Garrie Chubb, Manager/Asset Performance; Boon Thiow, Manager/Management Accounting and Systems Executive Audit and Risk Committee and Board Audit and Risk Committee
Approver:	The Board and Peter McIntyre, Managing Director

When referring to TransGrid's policies, frameworks, procedures or work instructions, please use the latest version published on the intranet.

Table of Contents

1. Purpose

Risk is the effect of uncertainty on achieving TransGrid's objectives. TransGrid undertakes risk management processes to understand the risks it faces and to manage and mitigate uncertainty to a tolerable level. This procedure details the system, including templates and terminology, used by TransGrid to manage risk. Effective risk management involves all staff in TransGrid and applies to all business activities. Successful management of risk can:

- Improve organisational performance and increase organisational resilience
- Reduce foreseeable threats to a level that TransGrid is willing to accept
- Enable TransGrid to maximise opportunities that may present themselves.

An effective risk management process is a cornerstone of good corporate governance, which supports management in the achievement of TransGrid's business objectives as well as ensuring that TransGrid remains relevant and resilient into the future.

2. Scope

This Risk Management Framework provides the structure and tools that will facilitate the use of a consistent risk management process, whenever decisions are being made in TransGrid. This framework must be applied consistently across all projects, functions, processes and activities at all levels of TransGrid to ensure resources to treat risks are applied efficiently and effectively.

Directors are ultimately accountable for the decisions made in TransGrid and therefore they need to know that the important issues are being managed and that TransGrid will achieve its objectives. The Board receive information on TransGrid's management of risk through reporting provided to the Board Audit and Risk Committee.

In addition, it is a NSW State Government requirement[1] that government entities have a Risk Management Framework in place. To meet these expectations and as a standard of good governance, TransGrid has introduced a system of risk management planning and monitoring, which is based on the standard AS/NZS ISO31000:2009 Risk Management-Principles and Guidelines.

3. Definitions

Term	Definition
Context	Describes the goals, objectives and depth of analysis for the area of review. It considers the external and internal environment in which TransGrid seeks to achieve its objectives.
Control	Measure that is modifying or treating a risk.
Control - Detective	A mechanism put in place to detect the occurrence or possible occurrence of an event e.g. reconciliation of general accounts

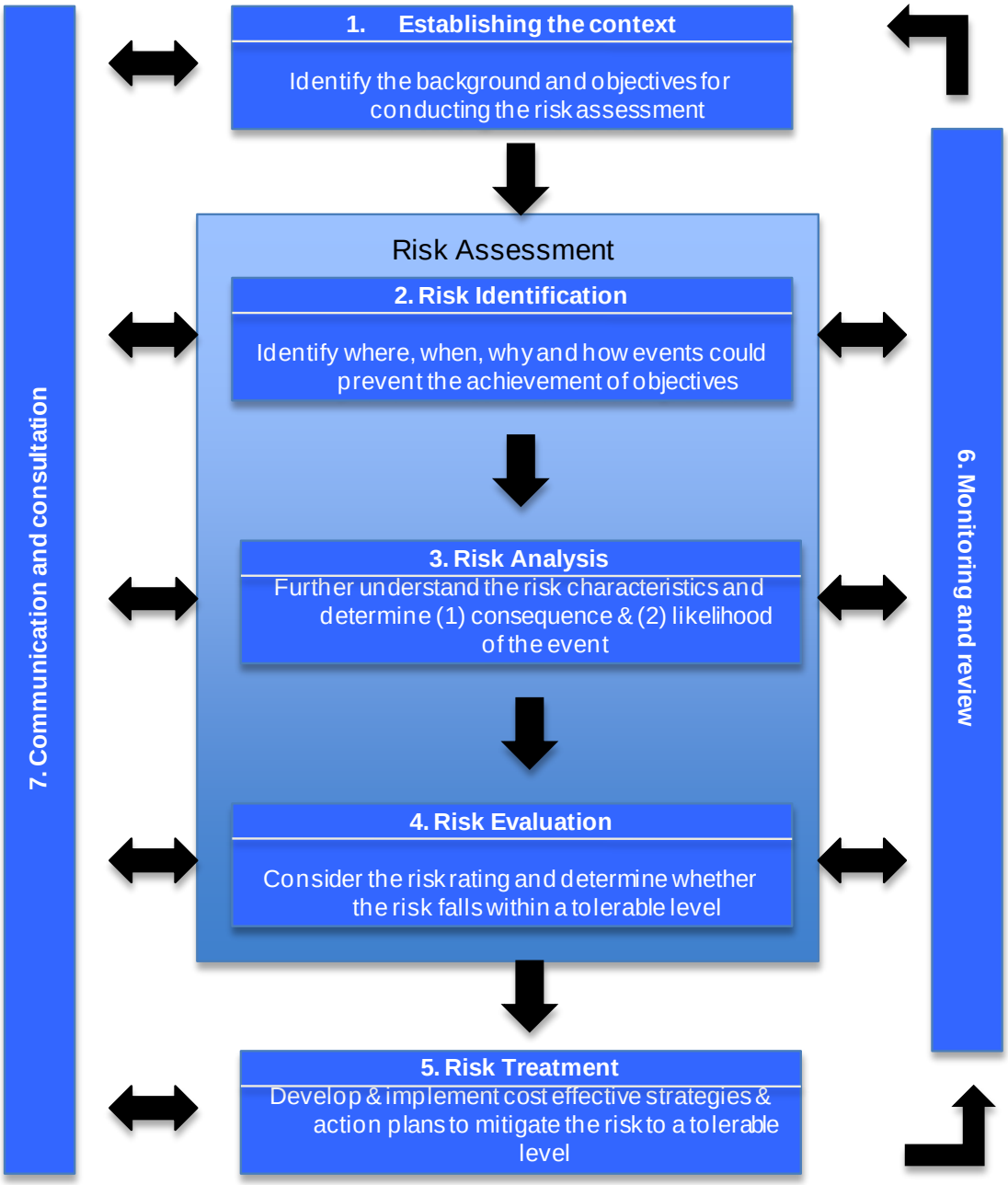
[1] Treasury Policy TPP 09-05, Public Finance & Audit Act 1983, Work Health & Safety Act 2011, Environmental Planning and Assessment Act 1979 and the Protection of the Environment Operations Act 1997.

Control - Mitigating	A mechanism put in place to respond to the impact in the event of a risk occurring and reduce the resulting impact e.g. business continuity plan.
Control owner	A control owner is responsible for the implementation of a control which mitigates a risk that they may not own e.g. Physical security is owned by Manager/Asset Performance but the majority of controls are owned by Regional Managers, such as providing local access cards.
Control - Preventative	A mechanism put in place to eliminate or reduce the risk from eventuating e.g. installing a fence around a substation.
Cost effective treatment	Cost effective describes actions that are good value, where the benefits and usage are worth at least what they cost to implement and maintain. A control is cost effective if the benefit is considered to be greater than the cost. The level of review and justification should be in proportion to the level of risk and proposed expenditure.
Inherent Risk	The level of risk that exists prior to control measures being introduced or applied, or the level of risk that exists if controls and risk treatments were removed or not applied.
Residual Risk	The level of risk remaining after control measures/treatments have been implemented.
Risk	The effect of uncertainty on achieving TransGrid's objectives. Risk is measured in terms of impact and likelihood. Uncertainty can have positive and negative effects on objectives.
Risk Assessment	A systematic process of risk identification analysis and evaluation.
Risk Consequence/Impact	The outcome of an event expressed qualitatively or quantitatively, affecting TransGrid's objectives. There may be a range of possible outcomes associated with an event; these could have a positive or negative impact on objectives.
Risk Event	An occurrence or change in a particular set of circumstances.
Risk Likelihood	The chance of something happening.
Risk Management	The culture, processes and structures that are directed towards realising potential opportunities whilst managing adverse effects. Risk management will provide greater assurance that TransGrid is achieving its objectives by minimising threats and seizing opportunities.
Risk Management Plan	A document, in the form of Attachment 1 - Risk Register Template which identifies risks, assesses their likelihood and consequence to derive the inherent risk, identifies current controls and management strategies, makes an assessment of the effectiveness of the existing controls, assesses the residual risk and identifies further risk treatments.
Risk Owner	The position with accountability and authority to manage a risk. For Key Risks across TransGrid, the assigned Executive General Manager will be the risk owner.
Risk tolerance	The level of risk TransGrid is willing to accept, which is in accordance with the risk appetite of the Board

Risk Treatment	Selection and implementation of appropriate actions or controls for modifying risk.

4. Risk Management Process Overview

Consistent with the AS/NZS ISO31000:2009, the TransGrid risk management process involves the following elements illustrated in the diagram below.



Adapted from: AS/NZS ISO31000:2009

A more detailed guide to the above steps is provided in **Section 5** **Risk Assessment Process**.

4.1. Risk Management Framework

The Risk Management Framework within TransGrid operates at two levels:

- Key Risks; and
- Operational Risks.

Key Risks

Key Risks are those risks that can impact the achievement of TransGrid's business objectives and corporate strategy. The Key Risk assessment is reviewed annually in its entirety as part of the corporate planning process and monitored quarterly by the Executive Audit and Risk Committee and the Board Audit and Risk Committee.

Operational Risks

Operational risks are those risks that occur as part of TransGrid undertaking its business and often feed into a Key Risk. These might include the risks associated with the achievement of project objectives and business as usual objectives. At the operational level there are a number of specific functional risk assessments undertaken including:

- Project
- Fraud
- Business Unit or Group
- Environment
- Health and Safety

As part of this framework, Business Units may develop specific policies or procedures for managing risk in an area of operation, for example Project Management, Environment, Work Health and Safety or Asset Performance. Specific procedures should only be developed where this procedure does not fully cover the requirement or further explanation is necessary.

Project risk assessment should be undertaken and reviewed throughout the life of the project. Group or Business Unit operational risk assessments are to be reviewed formally at least annually. Note that health and safety and environmental risk assessments are to be performed in accordance with TransGrid procedure - H&S Risk Assessments and TransGrid procedure - Identification of Significant Environmental Aspects. The Fraud Risk Assessment is undertaken in accordance with TransGrid's Corporate Governance Framework.

4.2. Risk Tolerance

Risk tolerance or risk appetite relates to the amount and type of risk that TransGrid is prepared to accept in pursuit of business operations and strategic objectives. Statements of risk tolerance assist management in assessing the appropriate level of controls to mitigate risks.

Risk tolerance levels are defined for different areas of operations and quantified by the Board in the "Overarching statement of TransGrid's risk tolerance" in **Attachment 2 – Qualitative Measure of Consequence on TransGrid**. Low level risks are generally considered to be at a level, which TransGrid can accept, however this may not be the case for areas such as safety of people, where TransGrid's tolerance is stated as "zero injuries and occupational illnesses".

In many instances some level of risk is unavoidable or encouraged, however the impacts of proposed actions and decisions should be properly identified, evaluated, communicated and managed to ensure that exposures are acceptable.

Not all risk management can be formalised and therefore considerable reliance is to be placed on the skill, experience and judgement of personnel to take risk-based decisions that are reasonable, justifiable and in line with the corporate objectives.

5. Risk Assessment Process

Detailed below are the generic steps that provide guidance for undertaking a risk assessment. The process does not necessarily have to be undertaken in sequence and for the review of plans some steps may not be required.

Risk Assessments should be undertaken by people who have detailed knowledge of the functional area being assessed, persons with overall responsibility and where practical a member of Corporate Audit and Risk Group.

Risk Assessments are judgmental in nature and are designed to direct attention to certain areas rather than be a precise quantification of any impact on TransGrid. For instance a risk that has minor impact, is unlikely to occur and is effectively controlled would not require any further treatment actions.

Step 1 – Establish the Context

Identify the background and objectives for conducting the risk assessment

The scope of the activity or decision, or parts of TransGrid to which this risk management process is to be applied should be established and the objective of that process or activity clearly understood, including its relationship to the overall business objectives. The assessment should be undertaken with consideration of the need to balance costs, benefits and opportunities. Inclusions, exclusions, assumptions and limitations should be articulated to ensure that all parties have a shared understanding of the area under review.

Without context the type or level of resources that should be assigned to manage the risk cannot be determined. For example, understanding key stakeholder expectations will influence the assessment of the consequences of certain events.

Step 2 – Risk Identification

Identify where, when, why and how events could prevent the achievement of objectives

Identify the risk source or uncertainty in achieving the objective, the cause and potential consequence. Risks may be identified from a review of hazards or vulnerabilities, or by the review of processes or functions and where they might impact the delivery of objectives.

Risk management is iterative; lists of risks will evolve over time.

- A template for registering risks is provided in **Attachment 1 - Risk Register Template**.

Step 3 – Risk Analysis

Further understand the risk characteristics and determine the consequence & the likelihood of the event.

While there is a subjective element to the assessment of risk, there must be a basis behind the assessment. Assumptions should be articulated and risk assessments documented to ensure accountability for the assessment is clear.

5.1. Assess inherent risk

Identify the risk and consequence inherent in what the area of the business is trying to achieve. At this stage the risk is considered without the application of controls or treatments, that is the worst-case scenario. The risk needs to be put into perspective. For example the risk of equipment failure in an environmentally sensitive area may be assessed as extreme when considered in isolation, however if there are only a small number of sites out of the total population which are within an environmentally sensitive area, then the likelihood of the risk would be reduced.

Assess the likelihood of the event occurring.

Likelihood	Frequency of occurrence
A. Almost certain	Likely to occur more than once every year. Expected to occur at least once a year; almost inevitable.
B. Likely	Likely to occur between once a year and once every 2 years. More than 50% chance of occurring in any year but unlikely to occur more than once a year.
C. Possible	Likely to occur between once every 2 years and once every 10 years. Less than 50% chance but greater than 10% change of occurring in any one year.
D. Unlikely	Likely to occur between once every 10 years and once every 33 years. Less than 10% chance but greater than 3% chance of happening this year.
E. Rare	Likely to occur less than once every 33 years. Less than 3% chance of happening this year.

When determining likelihood you should consider the frequency and exposure to the risk in the overall context of the total population, i.e. a daily action/task/event versus an annual or quarterly one, site specific risk versus state-wide. You should assess the likelihood and consequence together rather than select the extremes of each then combine them. E.g. starting a fire might be "likely" but consider starting a small fire versus a very large fire; would the large fire then be "unlikely" or "possible"?

Assess the impact if that event occurred. Assessments are qualitatively made on the basis of;

- Catastrophic
- Major
- Moderate
- Minor
- Minimal

A guide for assessing the impact on TransGrid is provided in **Attachment 2 - Qualitative Measure of Consequence on TransGrid**.

Make an assessment of the inherent risk using the risk matrix in **Attachment 3 – Risk Matrix**.

5.2. Identification and assessment of Current Management Strategies and/or Controls

Risks are rated on a scale from low to extreme as per the matrix in **Attachment 3 – Risk Matrix**. Generally no further action is required for low inherent risks, except to record and monitor them at least annually or whenever circumstances change. This process is performed as low risks can change in significance. In some instances low risks may be subject to excessive controls and this should be reviewed to ensure the appropriate balance of cost/benefit for risk and controls is in place.

For inherent risks rated **other** than Low, determine what management strategies and/or controls are in place to address the risks. Note: if an area of the business identifies a risk but cannot control the risk, then that area of the business is not the owner of that risk and they should notify the appropriate risk owner. If the area is a control owner for a risk owned in another group, or the risk is an input to a higher level risk this should also be noted on the risk register. This assists in providing a TransGrid-wide view of risks and controls.

The controls identified in treating the risks can be categorised into either preventative controls, detective controls or mitigating controls.

The type of control utilised would be dependent on the risk and the cost/benefit obtained from introducing such controls. Management must assess how effective and efficient these strategies and/or controls are in managing the identified risk. If controls are costly they may not be the most efficient way to treat the risk as the risk reduction may not justify the cost of control.

In some cases controls may need to be removed as too many controls may be inefficient and may stifle the achievement of business objectives. The level of control should reflect TransGrid's risk tolerance.

For risks with an extremely low likelihood but extremely high consequence (Black Swan risks) the decision to treat may not be justifiable on economic grounds but these risks may still be treated based on other grounds, such as stakeholder perceptions. These risks should be periodically reviewed to identify any changes in consequence and likelihood. This should especially be done after a major event in the electricity industry or elsewhere in the world.

The following table sets out a basis for measuring the effectiveness of controls.

Value	Qualification of the Effectiveness of Controls
Ineffective	The controls that have been applied are not adequate in treating the risk.
Partial	The controls that have been applied go part of the way to treat the risk or impact.
Effective	The controls that have been applied are value for money to treat the risk or impact.
Excessive	The controls that have been applied are more than necessary to treat the risk or impact and are not cost effective. There may be some over control here.

5.3. Assess the Current Residual Risk

Assess the residual risk taking into account the effectiveness of the current controls using the risk matrix in **Attachment 3 – Risk Matrix**.

The residual risk should not be higher than the inherent risk with the existing controls.

Having reviewed the risks with all the controls that currently exist then consider if certain controls are removed what impact occurs to the risk. If no change occurs then further investigation should be undertaken as there may be an over investment in the controls.

Step 4 – Risk evaluation

Consider the risk rating and determine whether the risk falls within a tolerable level.

Management should consider the residual risk level and determine if it falls within the tolerable level acceptable to TransGrid. As a rule of thumb if the residual risk or the assessment of the effectiveness of the controls results in either high or extreme residual risk then future management strategies and/or controls should be identified and implemented where they are cost effective. For medium level residual risk, management should consider whether controls or further treatment actions are necessary and/or cost effective. No further action is generally required for low inherent or residual risks, except to record and monitor them at least annually or whenever circumstances change.

For all risks the following risk treatments should be considered:

Acceptance where the level of risk is at a level acceptable to TransGrid. This generally occurs at the point where the cost of further treatment is greater than the benefit derived.

Avoidance refusing to accept the risk if it cannot be lowered by ceasing the activity where the risk occurs. This may not be the best alternative as a totally risk averse organisation will not grow and will generate a very low rate of return.

Reduction reducing the likelihood and/or consequence if it is feasible and cost effective.

Transference moving all or some of the risk to a third party. Transference of a risk does not mean the risk is entirely transferred but generally it is a partial transference through insurance coverage/contractual arrangements or some other means.

Increasing where the level of risk is assessed as too low and is inhibiting TransGrid's ability to achieve its objectives or the costs of controls do not match the benefits achieved.

Step 5 – Risk treatment

Develop and implement cost effective strategies and action plans to mitigate the risk to a tolerable level.

When choosing a treatment action, managers should also consider the cost of ongoing efforts and maintenance to ensure long-term viability. Sometimes a control with a high initial cost (e.g. an engineering solution) can be more cost effective in the long term than

one with a low initial cost that needs high levels of effort or ongoing maintenance (e.g. the development of procedures with associated training, supervision and enforcement).

A determination should be made as to what further treatment actions will be taken to mitigate the risk to a tolerable level. These actions should be documented in the risk plan and/or Business Unit plan to enable monitoring of their status and effectiveness at treating the risk. Treatments should be actioned in accordance the timeframes in **Attachment 3 – Risk Matrix**.

Step 6 – Monitor and Review

Risk Management Plans should be monitored regularly and formally reviewed at least annually or when a change in circumstances occurs.

Monitoring of risks and treatment actions should be undertaken regularly to ensure risks remain within the tolerable level and that treatment actions have been implemented and are effective. Key risk indicators (KRIs) should be developed to monitor important risks. Refer to the risk reporting and escalation diagram below.

A formal review is to include;

- an reassessment of the inherent risk based on changes in the internal and external environment;
- assessment of any emerging risks;
- assessment of the effectiveness and efficiency of the application of controls and new treatment actions.

The assessment should be used for planning purposes as well as a management tool to direct resources and effort. Corporate Audit and Risk will use the risk plans in the development of audit plans and will test the identified controls from the plans against actual activity. Differences will be identified in relevant audit reports and the risk plans should be updated by the officers responsible for the risks and forwarded to Corporate Audit and Risk.

6. Risk Reporting and Escalation

Residual risks are to be actioned in accordance with the following diagram. When a risk is identified it should be notified/escalated, based on its residual risk rating, to the appropriate level of management. That manager should assess whether the risk is mitigated to a level that is within TransGrid's risk tolerance, considering the cost and effectiveness of controls and the residual risk consequences. If the risk is within a range that is tolerable to TransGrid, then the risk is approved, included in a risk register and periodically monitored for any changes in the risk profile.

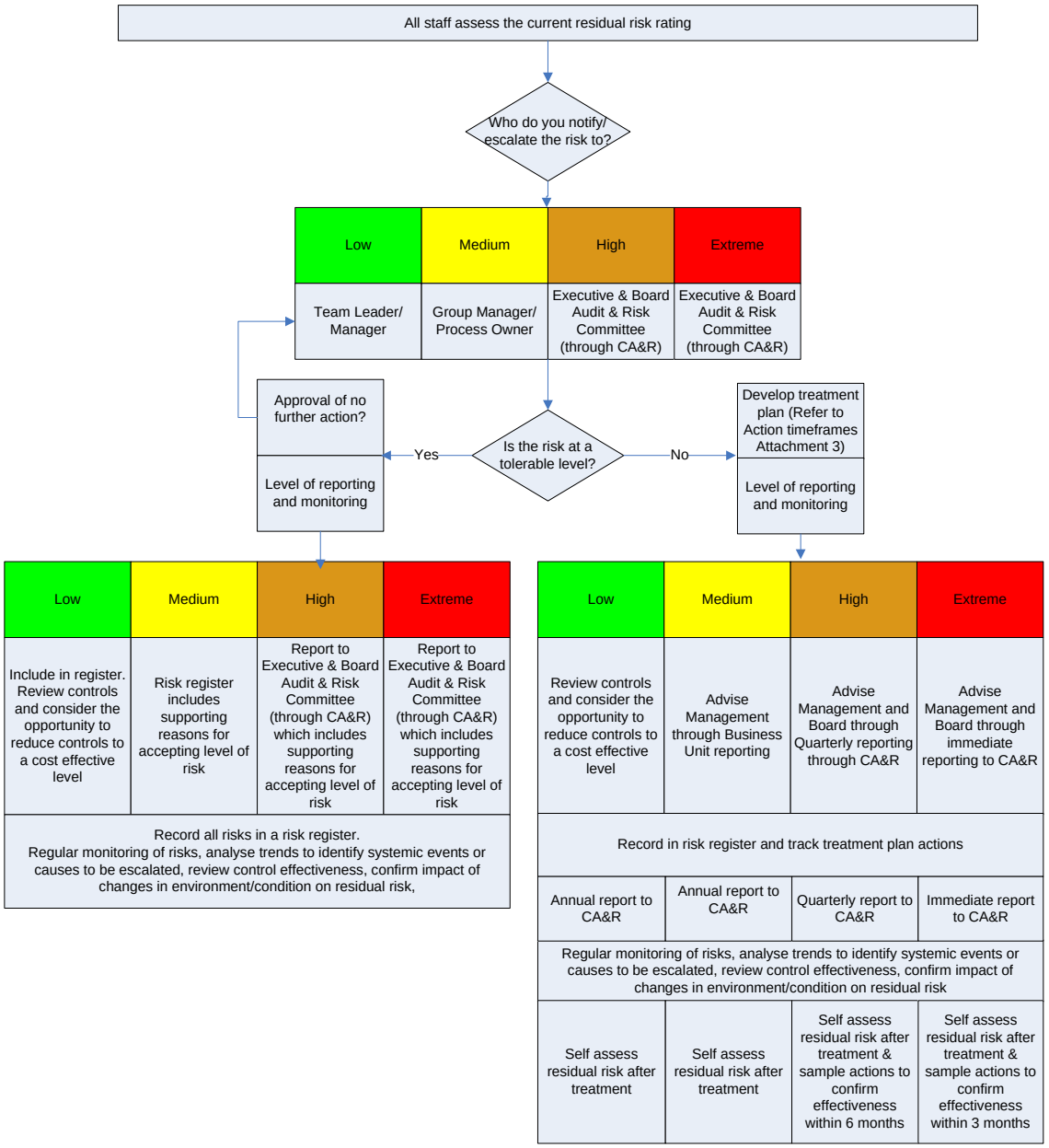
If the risk is not considered to be within TransGrid's tolerance, then the risk should be recorded, treatment plans developed, implemented and monitored.

Monitoring should identify when risk levels increase due to changes in the environment or controls are ineffective. If risk ratings increase then those risks should be escalated in accordance with the diagram below. Risk or control owners should undertake a review of the residual risk when treatment actions are implemented to assess whether the action was effective.

An example of a documented risk assessment is provided in **Attachment 4 – Sample Assessment**.

Risks are to be reported in the templates supplied by Corporate Audit and Risk (available on the Wire) with updated copies being forwarded to Corporate Audit and Risk. Key risks and important operational risks will be monitored and reported using key risk indictors (KRIs). Corporate Audit and Risk will work with Executive General Managers to report on Key Risk KRIs. Operational KRIs will be monitored and reported by Business Units, with copies of reports to Corporate Audit and Risk. Project risks should be monitored by Project Managers and reported and escalated in accordance with the below matrix.

Monitoring and Reporting matrix



Step 7 – Communication and Consultation

Communication and consultation should take place during all stages of the risk management process. Internal and external stakeholders should be consulted to ensure that:

- The context in which TransGrid is operating is fully understood
- The interests of stakeholders are understood and considered
- All risks are identified
- Different areas of expertise are drawn on when analysing and evaluating risks and different views are considered
- Endorsement and support for risk treatment plans is secured.

Both internal and external stakeholders will be interested in information on how TransGrid is managing its risks. Different stakeholders will have different information needs, which influences the level and content of reporting in relation to risks.

Effective communication and consultation should take place to ensure that those accountable for implementing the risk management process and treatment actions understand the basis on which decisions are made, and the reasons why particular actions are required.

7. Accountability

Role	Responsibility
The Board	**Sets the overall risk tolerance for TransGrid and delegates the responsibility of managing TransGrid's risk to the Managing Director.** The Board approves the Risk Management Framework
Board Audit and Risk Committee	On behalf of the Board is responsible for: • Review and endorsement of the Risk Management Framework • Approval of the risk management programme; • Input to and approval of the Key Risk register, developed by the Executive Audit and Risk Committee; • Oversight of the processes by which risks are managed including: o articulating the overall risk tolerance levels; o monitoring TransGrid's risk management performance; o monitoring the Key business risks.
Board Health and Safety Committee	On behalf of the Board is responsible for: • Monitoring TransGrid's Health and Safety risks and performance; • Ensuring TransGrid implements processes for complying with duties under the Work Health and Safety Act.
Board Regulatory Committee	On behalf of the Board is responsible for: • Monitoring TransGrid's risks and performance in relation to revenue reset;

	• Preparing, verifying and signing off on the TransGrid's Revenue Reset proposal.
Board Remuneration and Structure Commitee	On behalf of the Board is responsible for: • Determining the remuneration and employment conditions of TransGrid's Executive and Senior Management and reviewing the organisational structure of the Corporation to support the delivery of TransGrid's business objectives.
Executive Audit and Risk Committee	Is responsible for: • Ensuring implementation of controls and management of risks; • Integrating risk management into the business planning processes and business decision making; • Leading the periodic review of the Key Risk assessment; • Endorsement of TransGrid's risk management process; • Monitoring TransGrid's risk management performance; • Monitoring the Key business risks and escalated operational risks; • Monitoring the status and effectiveness of treatment plans for Key business risks and escalated operational risks.
Executive General Managers/General Managers	Are responsible for: • Implementing controls to manage risks; • Review and oversight of their Business Unit's risk management plans; • Review and oversight of owned Key Risks and operational risks; • Monitoring the ongoing implementation, effectiveness and efficiency of risk control measures; • Implementing risk treatment actions identified in risk management plans; • Reporting on the status and effectiveness of treatment plans and escalating risks where appropriate.
Corporate Audit and Risk Manager	Is responsible for: • Facilitating the reviews of the Key Risk assessment and Business Unit operational risk assessments (at least annually); • Development, implementation and review of TransGrid's risk management process; • Provision of risk management advice and training; • Facilitating the identification of operational risks through Project and Fraud risk assessments as required; • Reporting on key risk indicators, treatment plan status and effectiveness, and escalated risks to the Executive Audit and Risk Committee and the Board Audit and Risk Committee; • Undertaking internal audits and implementing other monitoring to assess the efficiency and effectiveness of controls implemented by management.
Managers and Team Leaders	Are responsible for: • Identifying risks; • Management of risks, including the establishment of risk management plans;

	• Maintaining risk management plans, monitoring risks and controls and the monitoring status of treatment actions; • Reporting and escalation of risks as appropriate; • Undertaking monitoring to assess the efficiency and effectiveness of controls implemented • Applying a risk management focus in making business decisions.
Process Owners	Are responsible for: • Identifying risks within processes; • Determining and implementing appropriate process controls that will balance the cost of the controls with the risks, as per the Sub-delegation of Business Process Responsibilities procedure.

All Staff	Are responsible for: • Applying a risk management focus to their actions and business decisions; • Raising risks with their Manager or Team Leader for assessment and management as appropriate; • Undertaking their work in accordance with TransGrid's policies and procedures, as they describe many of the controls in place to mitigate TransGrid's risks.

8. Implementation

This procedure will be implemented through:

- Discussions when the Business Unit Risk Plans are facilitated;
- Updating of Corporate Audit and Risk page on the Wire;
- Maintenance of a Quick Guide for Risk Assessments available on the Wire; and
- Ongoing education and training by Corporate Audit and Risk group.

9. Monitoring and review

This procedure will be reviewed by the Executive Audit and Risk Committee in accordance with the standard schedule and when there are any major changes in the business to be taken into account.

10. Change history

Revision no	Approved by	Amendment
7	Board	Annual review 2014 – minor change
6	Board	Incorporating guidance from the NSW Treasury Risk Management Toolkit for NSW Public Sector Agencies. Update People consequence from HSEQ Audit findings – Holroyd July 2012. Update System Impact tolerance statement - EARC Clarifications for risk tolerance and cost effective controls or treatments
5	Managing Director	Simplification of process and consistent language to align with ISO 31000 7 step process.
5	Ken Carroll, Manager/Quality & Business Improvement	Reformat of procedure to revised template with the following minor amendment: • Removal of quality document numbers as they are no longer being used. • In 4.2, the link: Attachment 2 – Broad Areas of Consequence title amended to 'Attachment 2 – Qualitative Measure of Consequence on TransGrid'. • In 5., the link: 'Attachment 1 - Risk Management Plan Template' amended to 'Attachment 1 – Risk Management Assessment

		Template'.

11. References

AS/NZS ISO31000:2009 Risk Management-Principles and Guidelines

TransGrid Charter - Executive Audit and Risk Committee Charter

TransGrid Framework - Corporate Governance Framework

TransGrid Framework - Corporate Audit and Risk Framework

NSW Treasury - Treasury Risk Management Toolkit for NSW Public Sector Agencies (TPP 12-03a) August 2012

12. Attachments

Attachment 1 - Risk Register Template

Attachment 2 - Qualitative Measure of Consequence on TransGrid

Attachment 3 – Risk Matrix

Attachment 4 – Sample Assessment

Attachment 1 – Risk Register Template

Risk Description	Causes	Consequence/Impact	Inherent Risk			Control Description	Assessment of Control	Residual Risk			Person Accountable for Risk	Key Risk Indicators (KRI)	Targeted Risk Level	Further Risk Treatment	
			Likelihood	Consequence /Impact	Rating			Likelihood	Consequence /Impact	Rating				Further Risk Treatment	Timeframe for Further Actions

Attachment 2 – Qualitative Measure of Consequence on TransGrid

Broad Areas of Consequence						
Impact Description	**People**	**Operational/Compliance (Events not covered in the other columns)**	**Reputation (Including fraud and maladministration)**	**System Impact Assets/System Reliability and Availability**	**Environment**	**Financial (Excluding fraud & maladministration)**
Overarching statement of TransGrid's risk tolerance	Safety is our first priority and our goal is zero injuries and occupational illnesses. Working safely is a condition of employment and our people and contractors take ownership of safety by not accepting unsafe behaviour from anyone	TransGrid's actions ensure that there are no significant regulatory non-compliance findings made against the organisation and resources are available as required.	TransGrid has a duty to perform its business in the best interest of the state of NSW, therefore a positive organisational reputation is important to our standing in the community. TransGrid will not tolerate any instance of fraud or maladministration	TransGrid aims to provide a level of supply reliability that balances the cost of providing services with the value customers place on reliability of supply including the additional value customers place on avoiding low probability high consequence events.	TransGrid is committed to conducting its activities and services in a manner that minimises pollution and complies with relevant legislation, industry standards and codes of practice	Every employee should make decisions in a commercial way and spend money as if they own the business
Catastrophic - Impact affects the ongoing viability of TransGrid	Actual or potential multiple fatalities or single death caused by negligence of TransGrid or systemic failure	Event would have a significant impact on TransGrid's ability to achieve its corporate objectives, which may lead to an inability to operate in the longer term. Impact would require extensive organisational effort (diverted from business as usual) for more 3 months.	Would only result from events that are seen as extremely serious or catastrophic in the other areas of consequence.	Extended period or repeated loss of Supply to CBD or extended system "black start"	Repeated incidents or incident as a result of negligence causes significant harm and/or irreversible impact to World Heritage area, or species, populations or ecological communities identified as threatened. **Extent –** Widespread, on and off-site impacts. **Duration** – Long term, irreversible impacts.	Financial impact (expenditure of any nature including legal fees, labour costs associated with the incident) in excess of $500 million that would result in insolvency.[2]
Major – Impact is significant and medium to long term	Actual or potential fatality or extensive serious injuries leading to permanent total disability.	Major extended industrial or other disruption leading to inability to operate the business. Impact would require significant organisational effort for up to 4 weeks. Permanent loss of a significant amount critical data.	Extensive stakeholder and community outrage, with ongoing national media coverage leading to serious reservations being expressed about the organisation's ability to deliver its objectives.	Loss of Supply to CBD or event leading to system "black start"	Significant harm and/or irreversible impact to World Heritage area, or species, populations or ecological communities identified as threatened. **Extent –** Widespread, on and off-site impacts. **Duration** – Long term, irreversible impacts.	Financial impact (expenditure of any nature including legal fees, labour costs associated with the incident) in excess of $50 million, but less than $500 million.
Moderate – Impact is serious but short to medium term	Actual or potential serious injury with medical treatment required and significant lost time, permanent partial disability.	Industrial or operational disruption for an extended period. Impact would require extensive local effort for up to 2 weeks. Significant non-compliance that results in a major fine to TransGrid, director or staff member. Major prosecution or restriction put on TransGrid. Short term loss of critical data or critical ICT outages for extended period. Extreme customer dissatisfaction or multiple complaints to regulator.	Extensive stakeholder and community outrage, with one-off national or ongoing local media coverage. Findings of systemic serious corruption resulting in stakeholder outrage, ongoing media coverage and significant loss of staff.	Unable to transmit energy for an extended period to a significant geographical part of the network or loss of load of 30MW or more for 6 plus hours. Extensive damage to multiple assets rendering them unusable in the medium term.	Significant impact on ecosystems (e.g. major fish kills, widespread death of flora/fauna, etc.) or destruction of area of high cultural heritage (European or Aboriginal heritage). **Extent –** Local, on and off-site impacts. **Duration –** Medium to long-term impacts. Potentially reversible over a duration of several years.	Financial impact in excess of $5 million but less than a $50 million.
Minor – Impact is limited and short to medium term	Medical treatment required and lost time.	Regulatory non-compliance resulting in sanctions/penalties by a Regulatory Authority. Prolonged or multiple customer complaints or dissatisfaction, complaints to regulator. Short term critical ICT system unavailability.	Significant event, which would require some management effort to recover standing. Limited community dissatisfaction, local media coverage. Findings of serious corruption against several members of staff.	Failure of supply greater than 0.4 system minutes. Extensive damage to key asset rendering it unusable in the short term.	Moderate impact on ecology (e.g. Small PCB oil spill with some discharge offsite) or damage to area of cultural heritage (European or Aboriginal heritage). **Extent –** Local, primarily on-site impacts with possible minor impacts on adjacent areas. **Duration** – Short to medium term, generally reversible impacts**.**	Financial impact in excess of $500K but less than a $5 million.
Minimal – Limited immediate impact	Incident requiring first aid, no lost time, near miss.	Regulatory non-compliance resulting in notification by a Regulatory Authority. Short term general ICT system unavailability.	Consequences can be readily absorbed but management effort would be required to minimise impact. Limited community dissatisfaction. Finding of corruption against a staff member.	Failure of supply less than 0.4 system minutes but greater than 0.05 system minutes. Damage to key asset(s) able to be addressed with no significant impact on operations.	Moderate impact on ecology, nuisance impacts (e.g. odour) or minor damage to area of cultural heritage (European or Aboriginal heritage). **Extent –** Local impacts contained to site. **Duration –** Short-term reversible impacts.	Financial impact less than $500K.

[2] Business viability was considered as TransGrid remaining solvent i.e. the ability of TransGrid to access funds to meet liabilities on demand. The TCorp approved borrowing limit and the currently drawn down funds were considered in assessing the $500M threshold.

Attachment 3 – Risk Matrix

Likelihood/Consequence	Minimal	Minor	Moderate	Major	Catastrophic
Almost Certain	Low	Medium	High	**Extreme**	**Extreme**
Likely	Low	Medium	High	**Extreme**	**Extreme**
Possible	Low	Medium	Medium	High	**Extreme**
Unlikely	Low	Low	Medium	Medium	High
Rare	Low	Low	Medium	Medium	High

Residual Risk Action Timeframe

Extreme – Immediate action is required or contingency plans implemented to address any operational issues. A plan should then be put in place within 1 month to manage the systemic risk to an acceptable level.
High –Immediate response is required or contingency plans implemented to address any operational issues. A cost effective plan should then be put in place within 3 months to manage the systemic risk to an acceptable level
Medium – Risk will impact on TransGrid, but not as seriously as Extreme or High risks. Additional controls may require consideration but a cost benefit assessment should be undertaken.
Low – Low level risk which is generally considered to be at a level that TransGrid can accept

In the event that the residual risk remains at Extreme or High then these risks need to be communicated to the Corporate Audit and Risk Manager to inform Executive and Board Audit and Risk Committee for endorsement of the risk.

Attachment 4 – Sample Assessment

Risk Description	Causes	Consequence/Impact	Inherent Risk			Control Description	Assessment of Control	Residual Risk			Person Accountable for Risk	Key Risk Indicators (KRI)	Targeted Risk Level	Further Risk Treatment	
			Likelihood	Consequence /Impact	Rating			Likelihood	Consequence /Impact	Rating				Further Risk Treatment	Timeframe for Further Actions
Inefficient or ineffective delivery of TransGrid's work program	Lack of clarity in scope of project Lack of internal & external resources	Network reliability impacted Over budget	Likely	Moderate	High	Governance process and subdelegations for approval	Partial	Possible	Moderate	Medium	EGM/CPD	% on time % on Budget	Low	Regular monitoring by PMO Resource plan	June December