Governance Institute of Australia Ltd

Risk Management Policy

1. Overview

Risk management is a key element of effective corporate governance.

In view of this, Governance Institute of Australia Ltd (Governance Institute) has developed a Risk Management Policy and Process not to completely avoid risk, but to identify and manage risk to assist in achieving desired outcomes in a properly informed way.

2. Background

What is risk?

There are a number of definitions of risk. Some examples are listed below:

- 'Risk is the effect of uncertainty on objectives.' (AS/NZS ISO 31000:2009)
- 'Risk is the combination of the probability of an event and its consequences.' (ISO/IEC Guide 73)

What is risk management?

As with risk, there are several ways of describing risk management:

- 'Risk management refers to the architecture (principles, framework, and process) for managing risks effectively.' (AS/NZS ISO 31000:2009)
- 'Risk management is the process whereby organisations methodically address the risks attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities.'

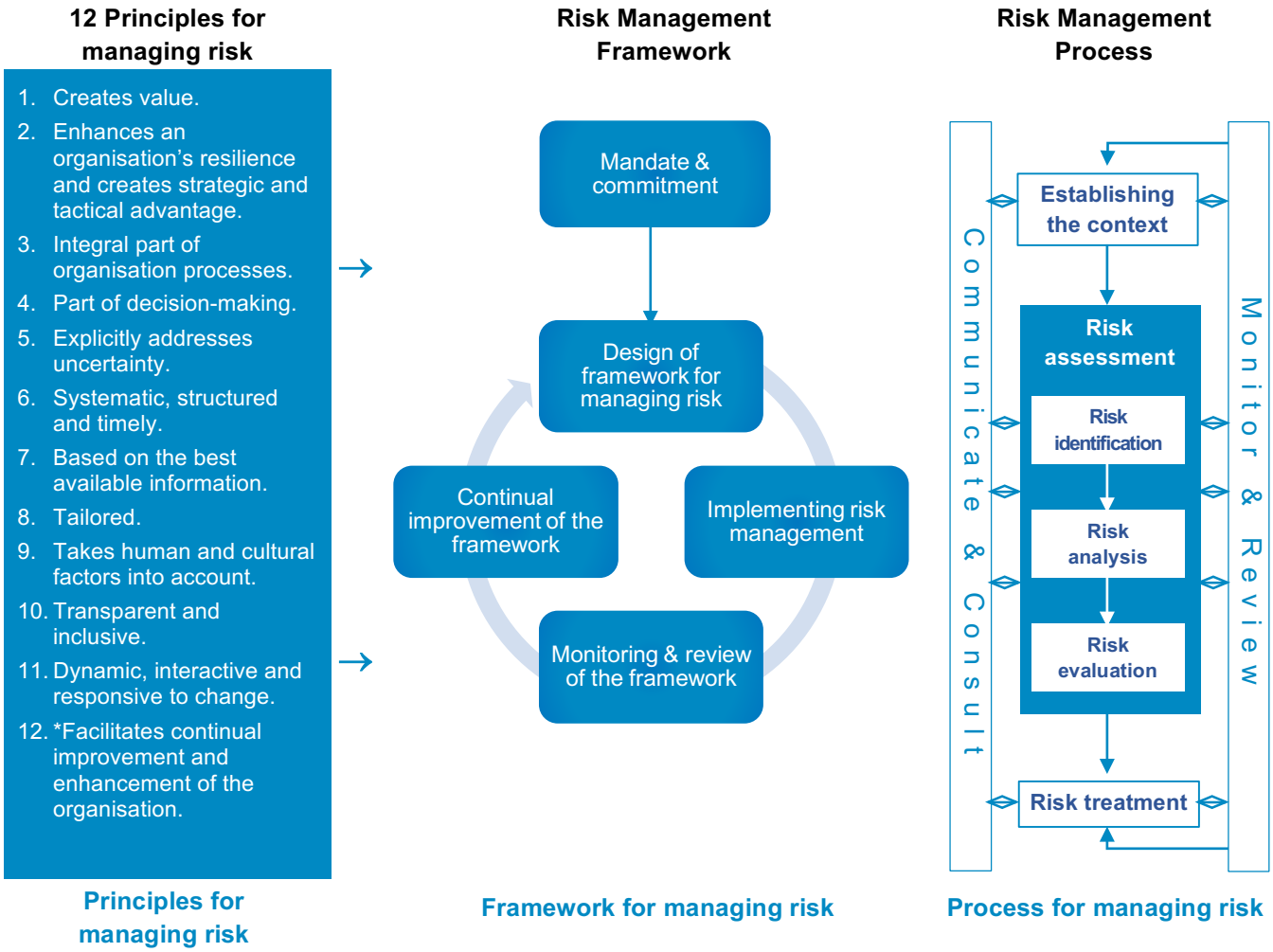
Risk management is increasingly recognised as being concerned with both the positive and negative aspects of risk. It marshals the understanding of the potential upside and downside of all those factors which can affect an organisation. It increases the probability of success, and reduces the probability of failure.

Governance Institute's mission

Governance Institute's mission is to be the expert leader in the promotion and application of the practice of governance to drive responsible performance for the benefit of organisations and the wider community.

Governance Institute recognises that the management of risk is a key element of sound governance and an important strategy for the achievement of the Governance Institute mission and supporting objectives.

Components of the Australian Standards



*AS/NZS ISO 31000: 2009 refers to 11 principles. The 12th principle comes from the Business Continuity Standard AS/NZS 5050:2010, which is aligned with AS/NZS ISO 31000

3. Governance Institute's Risk Management Framework

Governance Institute has developed and implemented a Risk Management Framework based on the principles of managing risk set out in the Australian Standards (AS/NZS ISO 3100: 2009 and AS/NZS 5050: 2010), and incorporating this Risk Management Policy, a Risk Management Process which includes a monitoring and reporting system, and a Risk Register.

Objectives of Governance Institute's Risk Management Framework

The key objectives of Governance Institute's Risk Management Framework are:

1. Enable consistent and systematic risk identification and management strategies to be implemented at national, state, and individual activity level, by Governance Institute's management.
2. Enable the identification and implementation of mitigation strategies and appropriate risk controls.
3. Improving the decision-making process.
4. Achieving a balance between realising opportunities to achieve goals and improve performance, while minimising the possibility of financial loss and other adverse impacts.
5. Providing a reporting framework to enable senior management and the Board to effectively monitor risk management within Governance Institute.

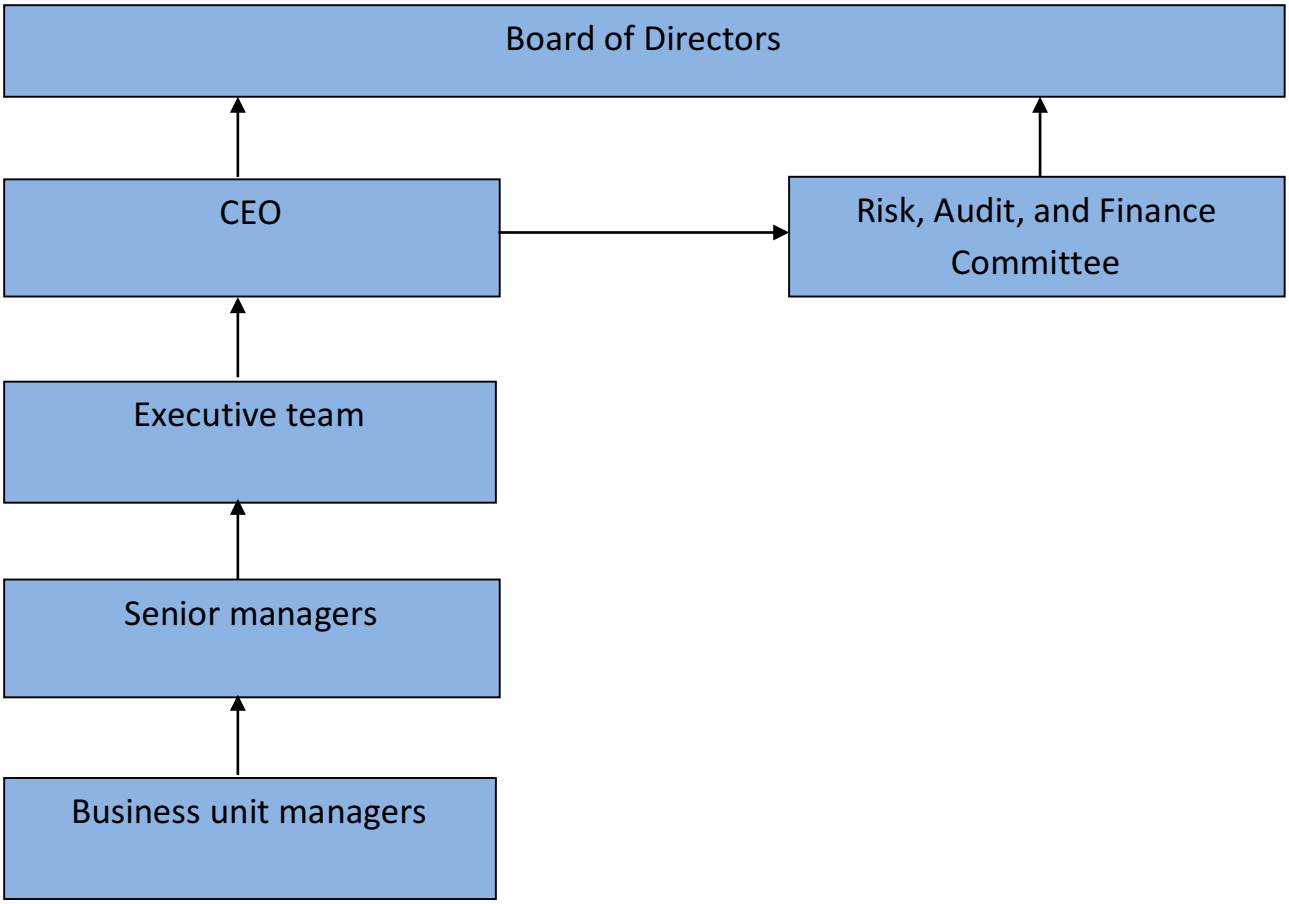
4. Responsibility

Governance Institute recognises that risk management is a 'whole of organisation' process that is applied by management to all levels of activity across Governance Institute.

The Board of Governance Institute is accountable to members for the effective implementation and monitoring of the Risk Management Policy and Process.

The Risk, Audit, and Finance (RAF) Committee is responsible for assisting the Board in the discharge of its responsibilities. The RAF Committee will oversee the development and maintenance of the Risk Management Policy and Process, and periodically review the Risk Register.

The management of Governance Institute is responsible for effectively integrating the Risk Management Policy and Process in to all its activities, and KPI's.



Risk management principles

Governance Institute's Risk Management Framework applies the principles for managing risk set out in the Australian Standards (AS/NZS ISO 31000:2009 and AS/NZS 5050: 2010) as shown below.

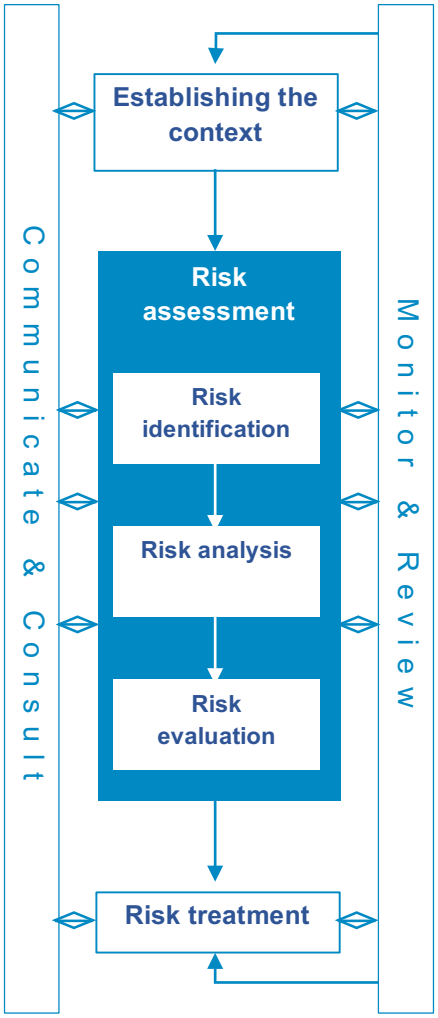
	Principles for managing risk	How Governance Institute applies these principles
1	Creates value	Risk management adds value to, and improves the success rate of Governance Institute's advocacy and educational and training offerings and helps maintain the viability and quality of its business.
2	Enhances an organisation's resilience and creates strategic and tactical advantage	The process for managing disruption-related risk involves anticipating rapid change, operating in non-routine modes and adapting to a changing environment within the context of our objectives. The experience of doing this enhances our adaptive capacity in that Governance Institute had developed a Business Continuity Program to manage the impact of changes.
3	Integral part of organisation processes	Risk Management is applied to Governance Institute's processes starting with strategic planning, through budgeting, to operations, and is embedded in staff KPI's and performance appraisals.
4	Part of decision-making	Governance Institute's decision-making is done against the background of known documented risks in a risk register. The risk register, with mitigation strategies, is updated where necessary as decisions are made.
5	Explicitly addresses uncertainty	Governance Institute addresses uncertainty in the analysis and evaluation phases of its risk management process.
6	Systematic, structured and timely	Governance Institute has documented its Risk Management Policy and Process, and established a Risk Register. Management addresses risk in its decision-making and incorporates risk management into its performance appraisal. The RAF Committee periodically reviews risk management and reports to the Board.
7	Based on the best available information	Governance Institute uses historical data, experience, stakeholder feedback, observation, forecasts, and expert judgement in the Identification, analysis and evaluation phases of the Risk Management Process.
8	Tailored	Governance Institute's Risk Management Framework has been developed specifically for Governance Institute. Risks have been categorised by risk type, as well as by responsible manager.
9	Takes human and cultural factors into account	Governance Institute's Risk Management Framework has been developed to be easily understood by all levels of management within Governance Institute, and to be a benchmark in Governance Institute's promotion of effective governance.
10	Transparent and inclusive	Governance Institute's Risk Management Framework is widely available to all levels of management and the Board of Governance Institute. All managers are responsible for the management of risks within their area of responsibility and are evaluated accordingly against their KPI's. Risk is monitored and reviewed by the RAF Committee and the Board.
11	Dynamic, iterative and responsive to change	Governance Institute's Risk Register and risk mitigation strategies are regularly reviewed by responsible managers and through the performance appraisal process. Risk is reported up to the RAF Committee and Board, and feedback is provided at each management level. The Policy, Process and Register are subject to annual review by the RAF Committee.
12	Facilitates continual improvement and enhancement of the organisation*	The Risk Management Framework provides the assurance and confidence that management and the Board needs to develop Governance Institute's future strategies, and improve the operation of its business.

*AS/NZS ISO 31000:2009 refers to 11 principles. The 12th principle comes from the Business Continuity Standard AS/NZS 5050:2010, which is aligned with AS/NZS ISO 31000

Governance Institute of Australia Ltd

Risk Management Process (RMP)

Governance Institute of Australia Ltd's (Governance Institute) process for managing risk is based on the process in the Australian Standard, shown diagrammatically below.



Process for managing risk

1. Establishing the context

'*Establish the external, internal and risk management context in which the rest of the process will take place. Criteria against which risk will be evaluated should be established and the structure of the analysis defined*.'

Governance Institute promotes effective governance and administration which is a constantly changing scene at both national and international level. It is constrained by its ability to generate earnings from subscriptions, education, training, and events, and operates in competition with other professional associations and education providers.

As with any professional association the context of the process is wide as there are multiple stakeholders including members, staff, directors, state and national councils and active practitioners.

Senior staff in the organisation have substantial and clearly defined responsibilities, are highly professional and in a position to manage the risks that are within their area of responsibility. While there is substantial assistance given by committees of members, it is the senior staff that will carry prime responsibility to manage risks and report occurrences should they eventuate.

As Governance Institute's activities are as an education provider, publisher of intellectual property and advocate, the criteria for evaluating risks revolve around: financial impact, employee continuity, image, reputation and business continuity.

The RMP involves all senior staff, councillors and the Board in the identification of risks to provide a wide range of inputs. Subsequent to risk analysis, those risks with an extreme level of risk are reported to the RAF Committee and the Board.

To augment the internal risk management process the Board calls for an external risk review every [3] years that evaluates the risk position of Governance Institute at that time and in the context of previous reviews.

2. Risk identification

'Identify where, when, why and how events could prevent, degrade, delay or enhance the achievement of the objectives.'

Identifying risks and building a Risk Register for Governance Institute involves a comprehensive review by all senior staff. The risk review is undertaken on an individual basis and then in a group workshop. Following this, the Board provides input to ensure the Risk Register is exhaustive.

Risks included are those faced by Governance Institute:

- as a commercial entity,
- when providing services under the Service Agreement to the National Council and its sub-committees and
- as a result of any association with alliance partners and/or sponsors.

The Risk Register contains a listing of all risks, mitigation strategies, analysis, and reporting requirements. The Risk Register is available to senior staff, the Board and National Council.

The Board has identified the risks confronting Governance Institute which it has categorised as follows:

1. Reputation and strategic risks
2. Strategic market product/Development risks
3. Chief Executive's office
4. Business continuity management (BCM) risks
5. Finance & administration
6. Policy
7. Publishing
8. Education & training
9. Marketing
10. Membership
11. State service delivery

3. Risk analysis

'Identify and evaluate existing controls. Determine consequences and likelihood and hence the level of risk. This analysis should consider the range of potential consequences and how these could occur.'

Given the nature of Governance Institute's business and its relatively small size, analysis is undertaken via input from internal and external stakeholders — staff, councillors and the Board — on a qualitative basis.

Qualitative analysis is appropriate for Governance Institute given the historical regularity of income streams, the extent of the governance processes in place across all major business units, the sophistication and reliability of management information systems and the high degree of linkage of the performance management system to all levels of staff.

Based on a qualitative analysis by all stakeholders a rating of the likelihood of an occurrence, and a rating of the consequence of that occurrence, is determined. An overall level of risk for that individual risk is obtained by multiplying the two ratings together.

The definition of likelihood and consequence ratings is outlined in the following two tables.

Likelihood rating

Risk rating	Description
A. Almost certain	Not unusual to happen. • Risk has more than a 90% chance of occurring; or • It is almost certain to occur in the next three (3) months.
B. Likely	Known to occur or has happened in the past. • Risk has 60–80% chance of occurring; or • Is likely to occur in the next six (6) months.
C. Possible	May occur. • Risk has a 30–60% chance of occurring; or • May occur within one (1) year.
D. Unlikely	Not likely to occur. • Risk has 5–30% chance of occurring; or • May occur within the next three (3) years.
E. Rare	May occur in exceptional circumstances (would be considered highly unusual). • Risk has less than 5% chance of occurring.

Consequence rating

Rating	Impact area	Description
Catastrophic	Life/Health	• Death or permanent serious disability. Unlikely to be able to return to work.
	Physical assets	• Total loss of buildings, plant and equipment, records.
	Non-physical assets	• Total loss of all electronic data and work in progress.
	Business interruption	• Extended interruption, more than three (3) months, full recovery unlikely.
	Reputation/Market share	• Extended national media attention. Irreparable damage. Major customers lost to competitors.
	Financial assets	• Financial failure of Governance Institute.
Major	Life/Health	• Life threatening injury requires lengthy hospitalisation/rehabilitation. More than a month off work.
	Physical assets	• Extensive damage to property and equipment. Repairs difficult.
	Non-physical assets	• Loss of up to a year of data or work in progress.
	Business interruption	• Up to three (3) months. Significant long-term impact on profitability.
	Reputation/Market share	• National adverse media attention. Loss of major customers.
	Financial assets	• Major financial loss of 0.25% of annual turnover or more in a single event

Moderate	Life/Health	• Significant injury requiring hospitalisation. A week to 1 month off work.
	Physical assets	• Significant damage to property and equipment. Repairable.
	Non-physical assets	• Loss of up to a month of data/work. Mostly recoverable.
	Business interruption	• More than a week. Probably long-term impact on profitability.
	Reputation/Market share	• Medium-term adverse local media attention.
	Financial assets	• Moderate financial loss of 0.125% of annual turnover in a single event.
Minor	Life/Health	• Injury requires a doctor. Less than one (1) week off work.
	Physical assets	• Minor damage. Repairable.
	Non-physical assets	• Loss of up to a1 week of data/work. Most recoverable.
	Business interruption	• 1 week or less. Minor long-term effect.
	Reputation/Market share	• Short-term adverse local media attention. Limited effect on market share.
	Financial assets	• Minor financial loss up to 0.0625% of turnover in a single event.
Insignificant	Life/Health	• Slight injury requires first aid only. No lost time.
	Physical assets	• Localised damage, easily repaired.
	Non-physical assets	• Fully recoverable loss of 1 day's data or work in progress.
	Business Interruption	• Minimal. No long-term effect.
	Reputation/Market Share	• No adverse media reports. No loss of market share.
	Financial Assets	• Insignificant financial loss

4. Risk evaluation

'Compare estimated levels of risk against the pre-established criteria and consider the balance between potential benefits and adverse outcomes. This enables decisions to be made about the extent and nature of treatments required and about priorities.'

Governance Institute has adopted a tiered system of risk categories that define the level of management attention that is required and the level and time scale of the response and reporting that is required.

Setting the overall risk rating
The matrix used then categorises risk into four levels as follows: **E: extreme** **H: high** **M: moderate** **L: low**

Likelihood	Consequences				
	1.Insignificant	2.Minor	3.Moderate	4.Major	5.Catastrophic
A. (Almost certain)	M	H	H	E	E
B. (Likely)	M	M	H	H	E
C. (Possible)	L	M	H	H	H
D. (Unlikely)	L	L	M	M	H
E. (Rare)	L	L	M	M	H

Risk control effectiveness.

This is achieved by linking each mitigating strategy control using the following ratings:

Control rating	Definition
Excellent	• Highly dependable risk control process and procedures in place that can be relied upon to prevent risk materialising. • 90–100% effective.
Good	In most circumstances control will be effective to prevent risk event occurring or to mitigate risk in the event it does occur. • 80–90% effective
Satisfactory	Control is in place and works most of the time. Risks will be controlled most of the time. • 50–70% effective.
Poor	Control is in place, however, is considered to be generally unreliable or relatively ineffective. No guarantee risk will be controlled. • 20–50% effective.
Unsatisfactory	Control is totally ineffective. Risk will not be controlled. • Less than 20% effective.

In the event that a risk materialises that has been prioritised as high or extreme, the CEO must report the incident to the Chair of Governance Institute as soon as possible, advising:

- details of the incident or event;
- how the incident occurred;
- the source of the failure to prevent the risk occurrence;
- steps taken to minimise the impact of the occurrence;
- steps taken to rectify the breakdown or weakness in the risk controls systems; and
- that the adequacy of the Risk Register has been reviewed.

5. Risk treatment

'Where Governance Institute deems a risk to be unacceptable a range of treatment options are adopted involving multiple controls and selecting the most appropriate options to balance the cost of implementing against the benefits derived.'

A range of treatment options include changing the likelihood of occurrence, managing the consequences of the event should it occur, risk transfer (eg through insurance), and avoidance

These are achieved through the implementation of internal systems and controls, business continuity recovery plans, insurance, contractual arrangements and contingency planning.

6. Monitoring and review

'It is necessary to monitor the effectiveness of all steps of the risk management process. This is important for continuous improvement. Risks and the effectiveness of treatment measures need to be monitored to ensure changing circumstances do not alter priorities.'

Governance Institute's monitoring and review practices include the following:

- Continuous (or at least frequent) monitoring by operational staff and their manager through routine measurement or checking identified performance indicators, such as participant feedback at training events or retention rates of members.
- Reviews of risks and their treatments by internal directors and the CEO that are often selective in scope but typically routine and regular, such as exam sitting rates, completion rates or sign-off protocols with committees of members.
- Auditing, using both internal and external sources. These audits test systems and conditions. They are selective in scope and less frequent than the above measures and will use externally run surveys or consultants, such as the Beaton Consulting survey of member satisfaction or the periodic risk review undertaken by external auditors.
- Formal review of the Risk Management Framework by the RAF Committee, and formal reporting to the Board.
- Governance Institute uses a software program to manage and report on risks to assist reporting.

In addition, specific risk matters form part of the performance plan of all staff and are reviewed on a semi-annual basis by the CEO with internal Governance Institute directors and state managers, as part of the strategic planning and performance regime.

Formal risk assessments are conducted annually by the Board, usually at the last meeting of the year. This risk review forms the basis that they are satisfied with the Risk Management Framework in place and its effectiveness.

This process is coordinated and monitored by the Company Secretary.

7. Communication and consultation

'*Governance Institute is committed to clear communication and consultation at each stage of the Risk Management Program so that stakeholders' different views are integrated into the decision-making process.'*

This is achieved through*:*

- providing clear visibility to Governance Institute's Risk Management Program
- workshops
- induction training
- regular management and Board reporting