Risk Management Framework

1. Purpose and Scope

This Framework describes the mechanisms through which risk management is conducted by King's Own Institute (KOI). This framework supports the implementation of the Risk Management Policy.

The Framework sets out how risk management is embedded across KOI for all business operations and decision-making – across all levels of staff. It outlines the relevant components and arrangements that enable KOI to design, implement, monitor, review and eventually improve risk management across the organisation. The Framework includes:

- A summary of KOI's approach to risk management
- Details on the application of the framework
- Details on how KOI manages risks
- Details on KOI's risk culture
- Details on the management of the Framework
- A Summary of the key roles and responsibilities in managing risk.

This Framework applies to members of Council, committees and all staff.

2. Related Documents

This Framework is to be read in conjunction with KOI's:

- Risk Management Policy

3. Definitions

Risk	Risk is the effect of uncertainty on objectives, which refers to both the positive and negative impact of uncertainty. The level of Risk is measured in terms of Consequence and Likelihood.
Risk management	Risk management means a coordinated activity (or activities) to direct and control KOI with regard to risk.
Risk Management Action Plan	Risk Management Action Plan means a document maintained by the Compliance Manager on behalf of the Audit and Risk Committee through with the Committee can retain oversight of risk issues that are not already reported to the Committee through the reporting processes established by this policy.
Risk management framework	Risk Management Framework is the set of components that provide the foundations and organisational arrangements for designing, implementing, mentoring, reviewing and continually improving risk management throughout KOI.
Strategic Risk Register	The Strategic Risk Register defines the strategic risks facing KOI, and provides an assessment of mitigating controls and their impact upon inherent risks.
Major Project	A project that potentially has an impact upon the successful achievement of a strategic objective.

4. Applying the Framework

Risks need to be managed in the context of achieving organisational objectives and should include consideration of positive aspects of risk management (opportunities) as well as negative aspects (threats).

The framework is the primary source of guidance for staff in managing operational risk.

The framework has been designed to support staff to:

- understand how KOI identifies, responds to, and manages risk;
- understand the connection between the Risk Management Policy and Framework, Risk Registers and Risk Analysis Tools;
- understand, accept, and manage risk as part of their everyday decision-making processes.

Risk Appetite and Tolerance

Risk appetite is the amount of risk an entity is willing to accept or retain to achieve its objectives. It is a statement or series of statements that describes the entity's attitude towards risk taking.

KOI has a medium-risk appetite other than where regulatory compliance is required, in which case KOI has a low-risk appetite.

Risk tolerance is the level of risk taking acceptable to achieve a specific objective or manage a category of risk. Risk tolerance represents the practical application of risk appetite and is typically aligned to categories of risk such as strategy, financial or reputation.

While risk appetite usually contains qualitative statements, risk tolerance operationalises the statements by using quantitative measures where possible, to enable better monitoring and review. Risk appetite sets the tone for risk in general, whilst tolerance informs:

- Expectations for mitigating, accepting and pursuing specific types of risk;
- Boundaries and thresholds of acceptable risk taking;
- Actions to be taken or consequence for acting beyond approved tolerances.

Risk Culture

Risk culture refers to the shared attitudes, values and behaviours that characterise how an entity considers risk in its day-to-day activities. KOI aims to foster a positive risk culture. A positive risk culture promotes an open and active approach to managing risk – it considers both "threat" and "opportunity" and enables all staff to appropriately identify, assess, communicate and manage risk.

Senior management and other identified individuals are responsible for supporting a positive risk culture through initiatives and process. All senior staff should actively provide feedback on interactions with key stakeholders regarding areas of potential risk. It is important that all staff (including contractors) understand, accept and manage risk as part of their everyday decision-making process.

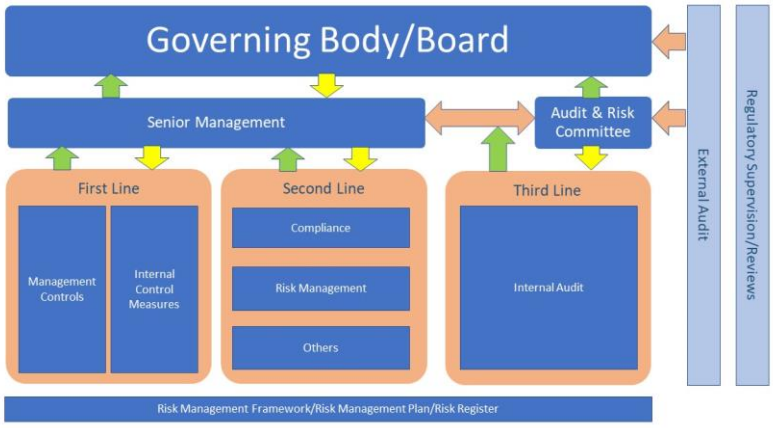
In order to maintain a risk culture:

- All staff and contractors should be familiar with KOI's approach to risk management and continually scan their environment for new risks and reassess existing risks relative to their environment, and report observations and suggestions to the relevant risk owner.
- All staff complete risk management training.

5. Framework

Overview

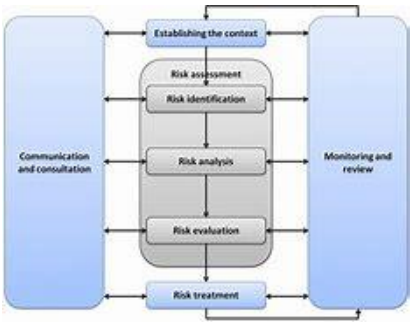
Risk management involves the entirety of KOI and its governance structure and is a shared responsibility of everyone within KOI as depicted in the "Three Lines of Defence" model below.



Risk Management Process

Risk Management is an iterative process, meaning that it is circular and that each iteration (or repeat) of the process is informed by the last one. This ensures that KOI is continually improving its management of risks.

The process is summarised in the following model (Source: Australia Standard for Risk Management (AS ISO 31000:2018):



Establishing the context involves analysing the internal and external context relevant to the activity or the risk. This should be done by or in consultation with a staff member or other individual who understands the contextual framework in which the activity would occur, if implemented (e.g. the TEQSA regulatory framework).

Risk Assessment involves considering the possible Risks of and to an activity, allocating each Risk a rating using set criteria (e.g. Council approved Risk Matrix and Descriptors) and evaluating whether the activity should be undertaken and any conditions that should be placed on it to try to avoid a risk altogether, or to reduce the likelihood or consequence of the risk if it occurs.

A Risk Assessment must be documented in writing for any activity that has the capacity to effect KOI's operations or ability to achieve its objectives.

Risk Treatment is the stage in which activities designed to manage the risk are implemented. There are many strategies that can be adopted to treat a risk including: avoiding it; implementing controls to decrease the risk's likelihood or consequence; transferring or sharing the risk (e.g. through contracts or insurance);

and deciding to accept and monitor the risk but preparing a contingency plan for potential use if the risk becomes more concerning in the future.

The ongoing appropriateness of the risk assessment and risk treatments are monitored throughout the life of the activity. The documentation and the risk treatments themselves may need to be amended or adjusted if risk context or ratings change, additional risks arise, risks are no longer relevant or risk Treatments are not effective.

Consultation and communication with stakeholders is essential to inform the establishment of context initially, allocation of appropriate risk ratings and identification of suitable risk treatments. Consultation with stakeholders is also necessary as well as to confirm the success (or otherwise) of the risk management process from alternative perspectives and to manage the stakeholder relationship on an ongoing basis.

Risk Matrix and Descriptors

Risk Rating Matrix

CONSEQUENCE	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
LIKELIHOOD					
Almost certain 5	M 5	S 10	H 15	E 20	E 25
Likely 4	L 4	M 8	S 12	H 16	E 20
Possible 3	L 3	M 6	M 9	S 12	H 15
Unlikely 2	L 2	L 4	M 6	M 8	S 10
Rare 1	L 1	L 2	L 3	L 4	M 5

LOW = 1 – 4; MODERATE = 5 – 9; SUBSTANTIAL = 10 – 14; HIGH = 15 – 19; EXTREME = 20 – 25

Risk Rating Descriptors

Rating	Description	Required Action
L (1 – 4)	Low	Acceptable: Unlikely to require specific application of resources. Manage by routine procedures. Monitor and review
M (5 – 9)	Moderate	Acceptable: Unlikely to cause much damage and/or threaten the efficiency and effectiveness of operations. Treatment plans to be developed and implemented by operational managers. Manage by specific monitoring or response procedures.
H (10 – 14)	High	Generally not acceptable: Likely to cause some damage, disruption or breach of controls. Senior management attention needed and management responsibility specified. Treatment plans to be developed and reported to relevant executive and/or CEO and President.
S (15 – 19)	Substantial	Not acceptable: Likely to cause a significant disruption to the effective functioning of operations, either financially or operationally. Immediate action required; must be managed by senior management with a detailed treatment plan reported to the relevant executive and CEO and President.
E (20 – 25)	Extreme	Not acceptable: Likely to threaten the continued effective functioning of operations or the survival of the organisation, either financially or operationally. Immediate action required; must be managed by senior management with a detailed treatment plan reported to the relevant executive, CEO and President and Council.

Risk Consequence Descriptors

Rating	Description	Health & Safety	Financial Impact	Business Interruption	Academic Performance	Reputation	KOI Objectives	Environmental	Regulatory
1	Insignificant	No injury but hazard identified	< $50,000 or <5% deviation from approved budget	No interruption to service. Inconvenience to operations.	<5% negative variation from performance KPIs	Negligible impact. Ad hoc mentions or rumours of a negative event on social media.	Resolved in day-to-day management. Negligible but has the potential to adversely impact key KPIs.	No lasting detrimental effect on the environment (i.e. harm, nuisance, noise, fumes, odour, o dust emissions of short term duration.	Minor non-conformance rectified internally. Correspondence with regulator acknowledging actions taken without further actions required. Internally identified non-conformance.
2	Minor	Minor personal injury; first aid required	$50,000 - $250,000 or 5% - 10% deviation from approved budget	Some disruption manageable by altered operational routine. Reduction in operational routine.	5% - 10% negative variation from performance KPIs	Adverse local and social media coverage for a brief time. Small pockets of possible student dissatisfaction.	Minor impact. <5% of key KPIs have a negative variation.	Short term, detrimental effect on the environment or social impact (e.g. minor discharge of pollutants).	One off non-conformance. KOI receives warning or other notice from regulatory authority to rectify non-conformance.
3	Moderate	Injury or illness; medical treatment required	$250,000 - $1 million or 10% - 15% deviation from approved budget	Disruption to a number of operational areas/campuses. Closure of an operational area/campus for up to one day.	10% - 20% negative variation from performance KPIs	Adverse media coverage by multiple outlets. Students and possible staff publicly express heir disapproval and disappointment in KOI.	Significant impact. 5% - 15% of key KPIs have a negative variation.	Serous discharge of pollutants or source of community annoyance that requires remedial action. Can be fully remediated.	Serious once off non-conformance resulting in imposition of conditions.
4	Major	Lost time injury or injury requiring hospitalisation and numerous days off work	$1 million - $5 million or 15% - 20% deviation from approved budget	Several key operational areas closed. Disruption to teaching/course schedules or key business activities for up to one week.	20% - 30% negative variation from performance KPIs	Adverse and sustained media coverage; public perception of KOI suffers. Possible calls for management reform and removal of some executives. Regulator publicly expresses concerns.	Major impact. 15% - 25% of key KPIs have a negative variation.	Long term detrimental environmental or social impact (i.e. chronic and/or significant discharge of pollutants. There will be some ongoing impact.	Systemic non-conformance resulting in suspension or withdrawal of approvals. Legal action taken against KOI and/or Council/its staff
5	Catastrophic	Fatality or permanent disability or ill-health	>$5 million or >20% deviation from approved budget	Disruption to services causing campus closure or key business closure for more than one week.	>30% negative variation from performance KPIs	Prolonged and adverse media coverage. Major student dissatisfaction; calls for regulator intervention; executives publicly criticised. Regulator considers cancellation of operating licences.	Disastrous impact. >25% of key KPIs have a negative variation. Abandonment of key strategic objectives.	Extensive detrimental long term ipacts on the environment and community (i.e. catastrophic and/or extensive discharge of persistent hazardous pollutant).	Major systemic non-conformance resulting in loss of TEQSA license, other key license or accreditation. Criminal proceedings and/or significant legal or regulator sanctions.

Risk Likelihood Descriptors

Rating	Description	Likelihood of Occurrence
1	Rare (<5% probability)	Highly Unlikely, but theoretically possible and may occur in exceptional circumstances. It could happen, but probably never will.
2	Possible (5% - 10% probability)	Not expected, but there is a slight possibility it may occur at some time during the cycle of the activity.
3	Occasional (10% - 25% probability)	The event might occur at some time during the life cycle of the activity, and/or there is a history of occasional occurrence at KOI or other tertiary education or similar institutions.
4	Likely (25% - 50% probability)	There is a strong possibility the event will occur as there is a history of frequent occurrence at KOI or other tertiary education or similar institutions.
5	Almost Certain (>50% probability)	Very likely. The event is expected to occur in most circumstances as there is a history of regular occurrence at KOI or other tertiary education or similar institutions.

6. Risk Reporting Processes

The following processes will be followed in collating and reporting risks.

Strategic Risk Reporting

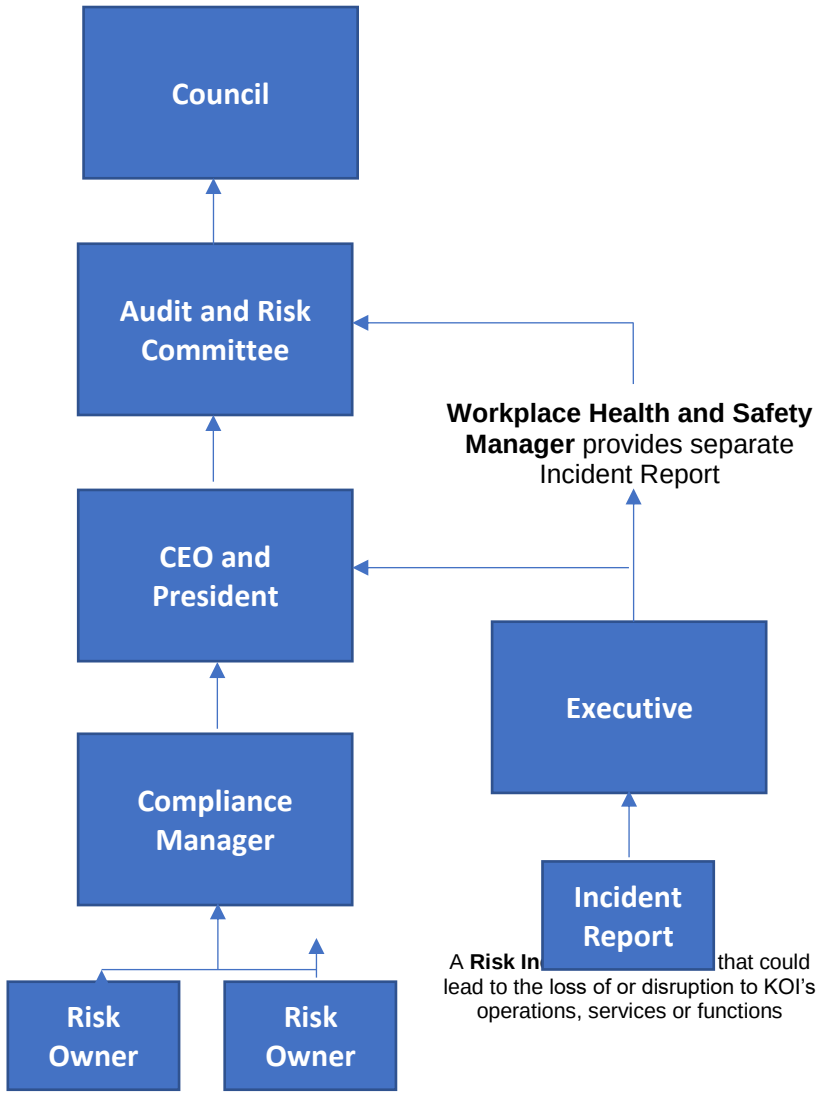
Chair, ARC reports to Council supported by the CEO and President

CEO & President presents Strategic Risk Management Report to ARC supported by the Compliance Manager

CEO & President advises Compliance Manager of risk incidents to be included in the Strategic Risk Management Report

Compliance Manager collates Strategic Risk Management Report based on input from Risk Owners and CEO & President

Risk Owners report against Strategic Risk Indicators in accordance with the schedule specified in the Strategic risk Register and advise of any risk incidents



Strategic Risk Register

New and Emergent Risk Reporting

Chair, ARC reports to Council supported by the CEO and President

CEO & President instructs Compliance Manager on new or emergent risks to be reported to each Audit and Risk Committee meeting

CEO & President considers escalated risks and directs response and/or distributes to Executive for action

Compliance Manager conducts preliminary enquiries and facilitates operational response, if appropriate, or escalates to the CEO and President with a recommendation as to action

Risk Owners/Staff Members who identify new or concerning risks can report to the Compliance Manager

Compliance Manager scans environment for new or emergent risks and changes to KOI's risk context or environment

A Risk Incident is an event that could lead to loss of or disruption to KOI's operations, services of functions

Strategic Risk Register Review

Council can endorse or provide feedback on the Strategic Risk Register

Chair, ARC recommends that Council endorses the Strategic Risk Register

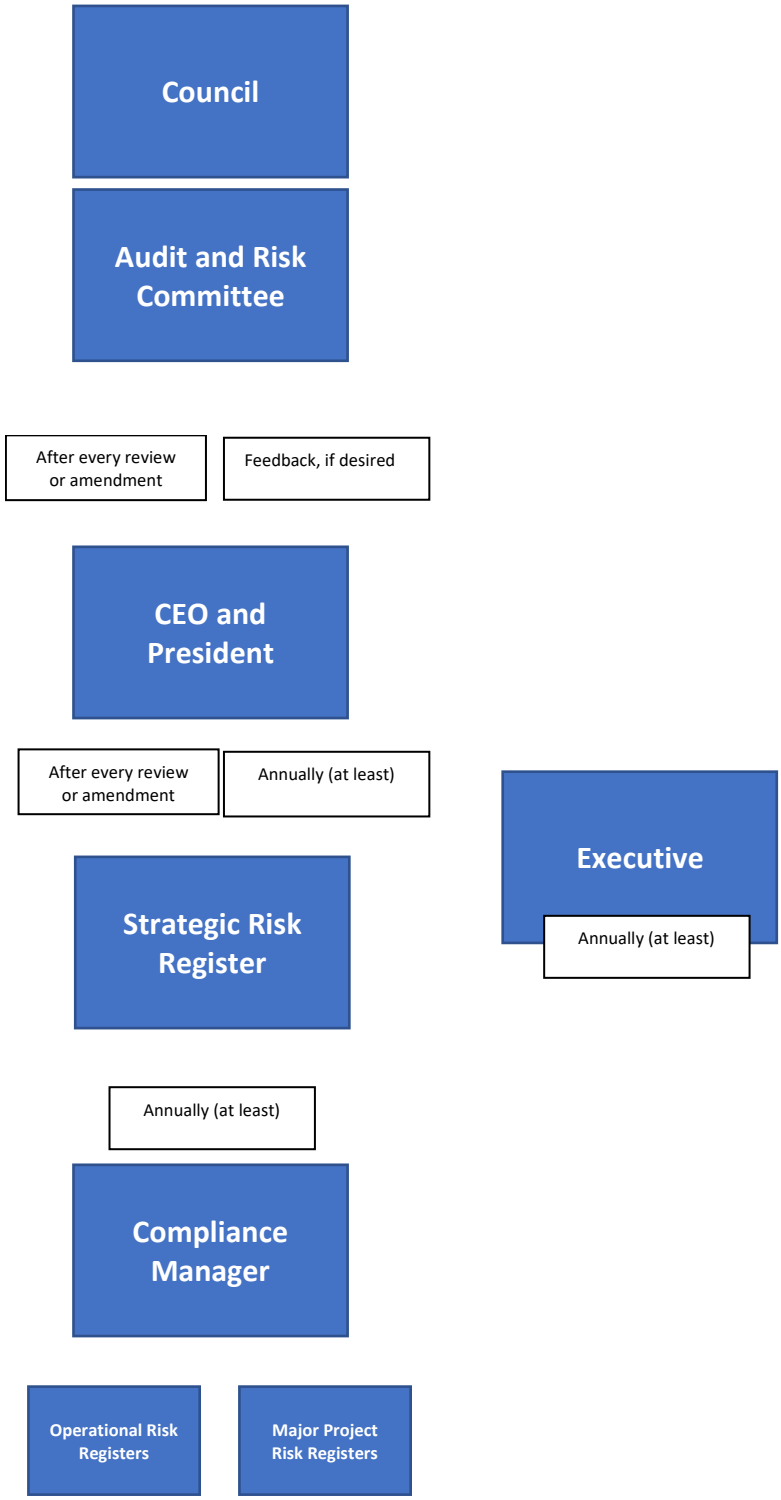
ARC provides feedback to the CEO and President on refreshed or amended Strategic Risk Register

CEO and President presents Strategic Risk Register to ARC after each review or amendment

Executive reviews at least annually and provides comment on Strategic Risk Register

Compliance Manager facilitates review of Strategic Risk Register at least annually

Risk Owners, Heads of work unit and Project Managers review, update and send risk registers to Compliance Manager at least annually



Procedures

KOI assesses risk using the Risk Matrix and Descriptors approved by Council.

Risks with the potential to affect KOI's ability to achieve its objectives must be managed using the risk management framework. Less significant risks may be managed using the whole or part of that process, provided that management of the risk is proportionate to the ability of the risk to cause harm to or promote the interests of KOI.

Information about risks and risk management must be reported to decision makers, advisers and oversight bodies through regular and ad hoc reporting channels as described in Risk Management Framework.

Risk Assessments and Management Plans

Wherever an activity, function or decision has the capacity to affect KOI's operations or ability to achieve its objectives, a risk assessment is required before a decision can be made on whether to proceed with or withdraw from the activity, or to escalate the risk.

The person or body responsible for the activity, function or decision must ensure that the risks involved are assessed, documented and managed in accordance with the Risk Management Framework. In the case of strategic risks, major project risks and other risks with the potential to affect KOI's ability to achieve its strategic objectives, this must also involve developing a written plan on how risks will be managed.

The Compliance Manager produce templates for risk assessments and management plans for use of KOI staff.

Operational and Major Project Risk Registers

Each work unit will maintain an Operational Risk Register comprised of risks to the work unit. Each risk in the Operational Risk Register must be allocated a risk owner responsible for managing, monitoring and reporting on the risk.

The project manager of each Major Project will maintain a register of risks to the Major Project, each allocated to a risk owner responsible for managing, monitoring and reporting on the risk.

The Compliance Manager at least annually collates all Operational and Major Project Risk Registers. The Compliance Manager will provide feedback to register-owners to ensure consistency in documentation and make recommendations to CEO and President about any risks they consider should be elevated to the Strategic Risk Register.

Strategic Risk Register

KOI will maintain a Strategic Risk Register comprised of risks to KOI achieving its strategic objectives. Each risk in the Strategic Risk Register will be owned by a member of the executive group who will be responsible for managing, monitoring and reporting on the risk.

The Strategic Risk Register will be developed in accordance with the process set out in the Risk Management Framework.

Risk Management Action Plan

The Compliance Manager will maintain a Risk Management Action Plan on behalf of the Audit and Risk Committee of risk issues of interest to the Committee that are not already reported on through the processes described in the Risk Management Framework. The Committee may specify, from time to time, any items to be added or removed from the Plan.

7. Roles and responsibilities

All KOI Persons are responsible for risk management and will comply with the Risk Management Framework, including the related policy. This includes:

- understanding KOI's objectives and the role that their work unit plays in achieving those objectives;
- understanding their role in KOI and the risk context relevant to that role;
- conducting proportionate risk management appropriate to their role; and
- escalating and reporting significant risks, or significant changes to the risk context, to their line manager or the Compliance Manager.

If a risk or risk management matter is escalated to a staff member, that staff member must provide timely feedback to the reporter about any action intended or taken on that matter.

All staff with line management responsibilities must ensure that risk management plays a role in performance management of direct reports.

Council

Council is responsible for overseeing KOI's risk management. This includes:

- developing and endorsing the Risk Management Framework;
- approving major decisions that may affect the KOI's risk profile or exposure; and
- annually endorsing the Strategic Risk Register.

Audit and Risk Committee

The Audit and Risk Committee's role and obligations are outlined in its Terms of Reference. Among other things, this involves:

- satisfying itself that KOI have appropriate strategies in place to manage their risks, and reporting its findings back to Council;
- considering reports and information from various sources about risk and risk management at KOI and reporting on those to Council;
- overseeing planning of internal audit activity, including approving the internal audit schedule; and
- providing strategic advice to the CEO and President about KOI's risk management.

CEO and President

The CEO and President is responsible for:

- ensuring that the Risk Management Framework is implemented, communicated and complied with;
- ensuring that a Strategic Risk Register is developed each time Council approves a new Strategic Plan and that the Register is reviewed, at least annually;
- overseeing management of strategic risks by members of the executive group and reporting on that to each Audit and Risk Committee meeting;
- proposing an internal audit schedule to the Audit and Risk Committee for consideration, having given due consideration to KOI's objectives and risks; and
- designating projects to be Major Projects and informing the executive group, the project manager and the Compliance Manager of that designation.

Executive Group

Members of the executive group are responsible for:

- managing, and reporting to the CEO and President on, any strategic risks that they own;

- responding to, and actioning (if appropriate), internal (and external) audit recommendations and items recorded in the Risk Management Action Plan; and
- ensuring that key strategic, operational and Major Project Risks within their areas of responsibility are identified, documented and communicated internally.

Heads of Departments

Heads of departments are responsible for risk management by their area of responsibility including:

- implementing, and ensuring compliance with, this policy within their area of responsibility; and
- maintaining an Operational Risk Register for their area of responsibility, that is continuously reviewed and sent to the Compliance Manager at least annually for collation.

Project Managers

Managers of Major Projects are responsible for risk management of their projects including:

- incorporating appropriate risk management into their project planning, activities and documentation; and
- maintaining a Risk Register for the project that is continuously reviewed and sent to the Compliance Manager at the commencement of the project and at least quarterly for collation.

Compliance Manager

The Compliance Manager is responsible for:

- managing the Strategic Risk Register process, as directed by the CEO and President;
- collating Operational and Major Project Risk Registers at least annually, providing register owners with feedback to ensure standardisation and making recommendations to the CEO and President about any risks that the Compliance Manager believes should be escalated to the Strategic Risk Register;
- providing tools, advice and support to facilitate effective risk management including:
    - monitoring and distributing information about KOI's risk environment to the executive group, Audit and Risk Committee and other internal stakeholders; and
    - maintaining risk registers, risk assessments and risk management plan templates;
- compiling, on behalf of the CEO and President, the executive group's update to each Audit and Risk Committee meeting about management of strategic risks;
- reporting to the Audit and Risk Committee on the Risk Management Action Plan and about any other relevant risk matters; and
- reviewing this policy and the Risk Management Framework in accordance with the requirements of this policy.

8. Associated Information

- Australia Standard for Risk Management (AS ISO 31000:2018)

Document control

Policy title	Risk Management Framework
Policy owner	CEO and President
Policy version date	25 November 2022
Policy approver	Council on the recommendation of the Audit and Risk Committee
Date of approval	12 December 2022
Date of Implementation	1 January 2023
Date of next review	1 July 2025for implementation 1 January 2026
Changes in this version	New Framework

KOI amends its policies periodically and printed copies of this document, either in part or whole, are considered as uncontrolled and should not be relied upon as the most current document. It is the responsibility of individuals printing the document to always refer to the KOI website for the current version.

**********END OF POLICY**********