Risk Management Policy

1. Purpose and Scope

This Policy establishes a robust framework for the identification, assessment, mitigation, and monitoring of risks that may impact King's Own Institute (KOI), its governance, academic and administrative operations, strategic objectives, and regulatory obligations. It ensures that risk is managed in accordance with the Australian Standard for Risk Management (AS ISO 31000:2018) and the Higher Education Standards Framework (Threshold Standards) 2021, specifically Standard 6.2 -- Corporate Monitoring and Accountability.

This Policy applies to the Council, all executive officers and staff, contractors, and any person with delegated risk-related responsibilities at KOI.

2. Related Documents

- KOI Risk Management Framework
- Risk Appetite and Tolerance Statement
- Strategic Risk Register
- Operational and Project Risk Registers
- Audit and Risk Committee Terms of Reference
- Internal Audit Strategic and Annual Plans
- Risk Assessment and Management Templates
- Business Continuity and Crisis Management Plans
- Student Safety and Wellbeing Policies
- Information Security Policy
- Delegations Policy
- Policy Management Policy

3. Definitions

Risk

The effect of uncertainty on objectives, whether positive or negative, measured in terms of likelihood and consequence.

Risk Management

A coordinated set of activities to direct and control KOI with regard to risk.

Risk Management Framework

The structured system of processes, tools, roles, and responsibilities used to integrate risk management into all organisational activities.

Risk Tolerance

The acceptable level of variation in performance relative to the achievement of objectives, representing the boundaries of acceptable risk-taking.

Risk Culture

The shared values, beliefs, attitudes, and practices that characterise how KOI considers risk in its daily activities and decision-making processes.

Strategic Risk Register

A register identifying significant strategic risks, their consequences, existing controls, treatment actions, and residual risk levels.

Operational Risk Register

A register of risks relevant to the functions and operations of individual departments or business units.

Major Project

A defined body of work with potential material impact on KOI's strategic objectives, regulatory obligations, or resource allocation exceeding $500,000 or involving significant reputational exposure.

Project Risk Register

A register of risks relevant to the planning, implementation and completion of a major project.

Risk Management Action Plan

A tool to assist the Audit and Risk Committee to monitor risk matters that require oversight outside the standard reporting mechanisms.

Key Risk Indicators (KRIs)

Metrics that provide early warning signals of increasing risk exposure in various areas of KOI's operations.

Risk Owner

The person or entity with the accountability and authority to manage a risk.

Three Lines Model

The risk management and assurance framework comprising: First Line (operational management), Second Line (risk management and compliance functions), and Third Line (internal audit).

4. Policy

Risk Management Integration

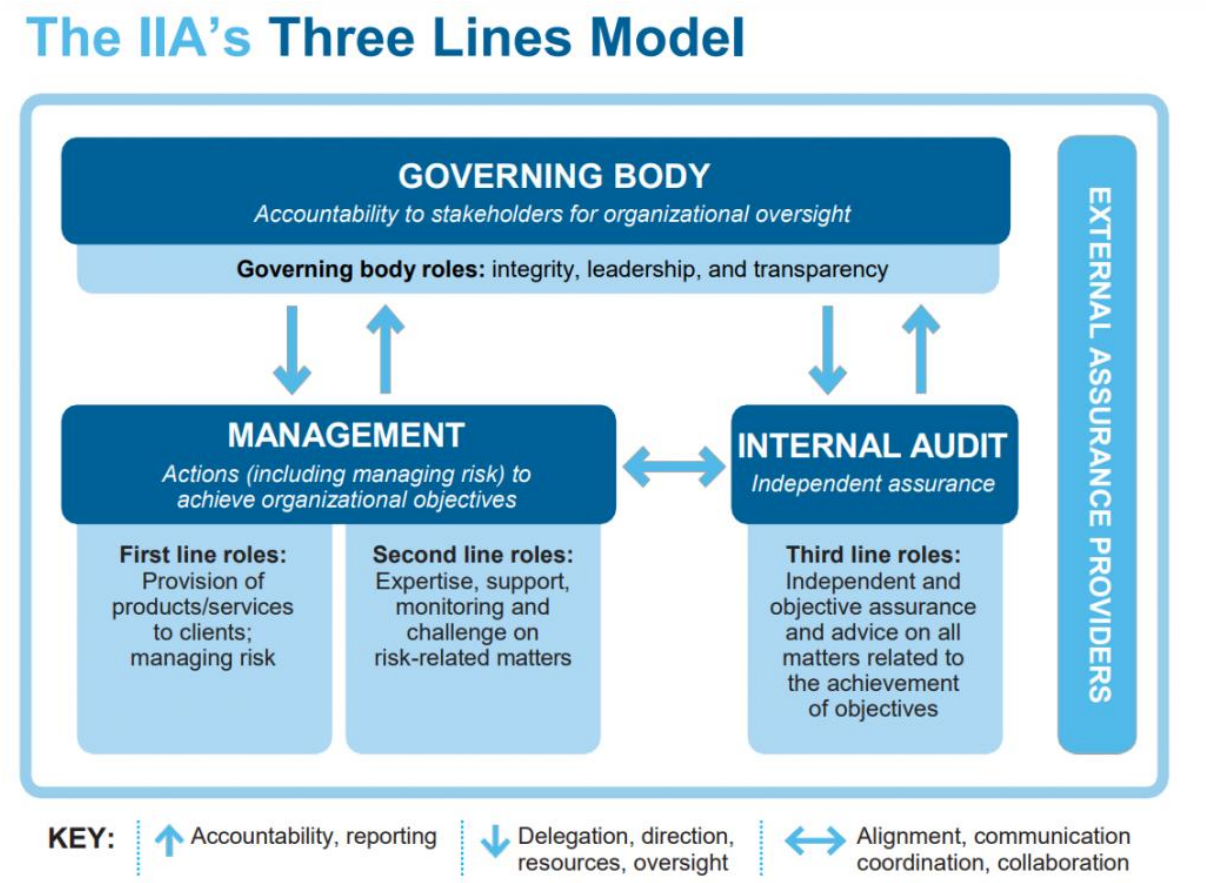
Risk management must be embedded into KOI's governance, planning, and operational processes and must be proportionate to the nature and severity of the risk.

All risks whether strategic, operational, financial, reputational, legal, regulatory, academic, technology, or environmental must be identified, documented, evaluated, and treated through consistent and evidence-based methods and in accordance with the Risk Appetite and Tolerance Statement.

Framework Implementation

The Risk Management Framework must be implemented in accordance with the Australian Standard for Risk Management (AS ISO 31000:2018) and incorporate the principles of the Three Lines Model published by The Institute of Internal Auditors.

The Risk Management Framework must be reviewed at least once every three years, or earlier if there is a significant organisational or regulatory change.



Risk Assessment Requirements

All activities that could affect KOI's capacity to fulfil its strategic or operational objectives must be subject to documented risk assessment using the Council-approved Risk Tolerance Statement.

Risk assessments must be conducted before major decisions are finalised, and risks must be escalated in accordance with defined criteria and thresholds.

Risk Treatment

For strategic risks and major project risks, written management plans are mandatory, including specific treatment strategies, assigned responsibilities, target completion dates, and monitoring arrangements.

Risk treatment options must consider accepting, avoiding, controlling/mitigating, or transferring risks based on their assessment against KOI's risk tolerance.

Risk Monitoring and Reporting

Key Risk Indicators must be established for significant risks to provide early warning of changing risk exposure levels.

Risk registers must be maintained, reviewed, and updated in accordance with specified frequencies and reported through appropriate governance channels.

Risk Culture and Training

All KOI personnel must understand risk in the context of the Risk Management Framework and Risk Tolerance Statement and actively participate in risk management within their areas of responsibility.

Mandatory risk management training must be completed by all staff within three months of commencement, with specialised training provided for risk owners and managers.

Crisis Management Integration

Risk management activities must be integrated with crisis management and business continuity planning to ensure effective response to risk events that threaten normal operations.

Third-Party Risk Management

Third-party relationships must be subject to appropriate risk assessment, including due diligence, contractual risk allocation, ongoing monitoring, and contingency planning.

Compliance and Performance

Compliance with this Policy is mandatory for all personnel within its scope, and non-compliance may result in performance management or disciplinary action.

The effectiveness of risk management must be measured through Key Performance Indicators, regular assessment of risk culture maturity, and tracking of risk treatment completion rates.

5. Principles

Risk management at KOI is guided by the following principles:

- Integration: Risk management is integrated into all organisational activities, governance processes, and decision-making;
- Structured: Risk management follows a structured approach that is systematic and tailored to KOI's context;
- Customised: Risk management is proportionate to KOI's external and internal context related to its objectives;
- Inclusive: Appropriate and timely involvement of stakeholders enables their knowledge, views, and perceptions to be considered;
- Dynamic: Risk management anticipates, detects, acknowledges, and responds to changes and events in an appropriate and timely manner;

- Best available information: Risk management explicitly considers any limitations and uncertainties associated with information and expectations;
- Human and cultural factors: Human behaviour and culture significantly influence all aspects of risk management at each level and stage;
- Continual improvement: Risk management is continually improved through learning and experience; and
- Transparency and accountability: Risk management approaches, processes, and outcomes are clearly communicated and subject to appropriate oversight.

Implementation and interpretation of risk management activities must ensure that:

- They are implemented in a fair and consistent manner, having regard to the principles and intent of this Policy;
- There is regard for the overall policy framework and the provisions of all relevant documents;
- Where an inconsistency arises, the higher order document prevails, or the approval authority must provide a determination; and
- Formal interpretation to address particular circumstances must be provided by the policy owner.

6. Roles and Responsibilities

Roles and responsibilities for implementing this Policy are outlined in the Risk Management Framework and associated procedures.

Risk Assessment and Management

All activities that could affect KOI's capacity to fulfil its strategic or operational objectives must be subject to documented risk assessment using the Council-approved Risk Tolerance Statement, Risk Matrix and Descriptors.

For strategic risks and major project risks, a written management plan is mandatory. Risk assessments must be conducted before decisions are finalised, and risks must be escalated as appropriate.

Registers

- Operational Risk Registers must be reviewed and updated at least annually and submitted to the Director, Risk and Governance.
- Major Project Risk Registers must be maintained throughout the life of the project and updated at least quarterly.
- Strategic Risk Register must reflect current priorities and emerging risks and be owned by Senior Executive Group members.

Risk Management Action Plan

The Director, Risk and Governance will update and maintain the Risk Management Action Plan to ensure the Audit and Risk Committee retains visibility of risks, including those not captured through regular registers. The Committee may amend its content as necessary.

7. Assurance Activities

Risk Management activities may be subject to internal or external audit.

8. Compliance with this Policy

Non-compliance with this Policy may result in internal review or disciplinary action.

Compliance with this Policy will be reported periodically to the Council via the Audit and Risk Committee.

9. Associated Information

- Australian Standard for Risk Management (AS ISO 31000:2018)
- Higher Education Standards Framework (Threshold Standards) 2021, Standard 6.2
- Three Lines Model - The Institute of Internal Auditors
- COSO Enterprise Risk Management Framework
- Committee of University Chairmen (CUC) Higher Education Code of Governance

Document control

Policy title	Risk Management Policy
Policy owner	CEO and President
Policy version date	29 August 2025 Version 2.0
Policy approver	AIBM Council on the recommendation of the Audit and Risk Committee
Date of approval	29 August 2025
Date of implementation	1 September 2025
Date of next review	29 August 2027
Changes in this version	Updates in terminology and rewording. Inclusion of reference to the "Three Lines Model" and the "Risk Tolerance Statement",