Risk Management

First Produced:	16/11/15	Authorisation:	Te Kāhui Manukura (TKM) Audit & Risk Committee Endorsement
Current Version:	01/12/25		
Past Revisions:	16/12/16, 27/06/17, 31/10/22		
Review Cycle:	3 years	Officer Responsible:	Director – Strategy, Planning, Performance
Applies From:	Immediately		

All policies on Waituhi are the current version. Please check date of this hard copy before proceeding.

1 Introduction

1.1 Purpose

The purpose of this policy is to provide clarity to Ara colleagues, the Ara Council, and contractors on their responsibilities of identifying, assessing, mitigating, monitoring, and reporting on risks.

1.2 Scope and Application

This policy applies to all Ara colleagues, the Council, and contractors in all areas of operations within Ara.

1.3 Formal Delegations

a Refer to CPP120 and CPP120a – Delegations Policy and Delegations Register.

1.4 Definitions

a **Risks**: uncertain future events that could impact on the organisation's ability to achieve its goals and objectives. Risk is assessed in terms of a combination of the impact and likelihood of an event occurring.

b **Key Risks:** risks that have a high impact and high likelihood of occurring. These are identified and reviewed quarterly by those in the Ara Council that make up Ara's Audit and Risk Committee.

c **Key Risk Register:** Ara Senior Management, the Council, and Audit & Risk Committee oversee the Key Risk Register, in relation to Ara's internal and external environment. In addition to that there are a number of other risk dimensions that have their own established procedures. They are –

i **Health and Safety** risks are managed through the Health and Safety Policy, and all associated Hazard & Risk Management procedures as managed by the Health and Safety Team.

ii **Financial risks** are covered by a CPP311 Treasury policy which considers financial and related risk. Ara makes conservative and prudent recognition and disclosure of the financial and non-financial implications of risks. Capital Works projects are managed through the Project Management Office. Post-project inception a risk workshop is held that establishes the initial risk register for a project. These are maintained by the external project managers and reported on monthly. Changes to risks are identified in the project progress report and discussed at the monthly Project Control Group meeting. For larger or more complex projects, specific risk workshops are held in order to have a major review of the risk register, this is also done at the start of the construction phase. A standard register format and scoring method is used throughout the projects.

iii **Information and Systems Strategy projects**, plus any other projects being managed by the Project Management Office, have a standard reporting framework. This

framework contains a risk register and for each project this is maintained from project inception and reported to the Project Control Group on a monthly basis.

d **Risk Management:** the process in which risk is managed. This includes risk identification, reporting, mitigation and allocating risk ownership.

e **Risk Management Procedures:** policies, processes, supporting templates, guidelines and forms that enable good risk management practice.

f **Internal controls**: processes, policies and procedures put in place by management to safeguard assets, promote accountability, increase efficiency and stop fraudulent behaviour.

g **Risk Ratings**: used to determine the likelihood and impact of an event occurring. The ratings are –

i **Extreme and Major**: serious risks that have a highly undesirable impact and high to certain likelihood of occurring. An extreme event would normally involve the Council management time. A major event would normally involve Chief Executive management time.

ii **Significant**: risks that will have an undesirable impact on the operational, reputational, financial or strategic effectiveness of the organisation and there is a high possibility of it occurring. A signification risk would involve Director management time.

iii **Moderate:** risks that may have an impact on the operational, reputational, financial or strategic effectiveness of the organisation and there is a possibility of it occurring.

iv **Minor**: risks that have a minimal impact on the operational, reputational, financial or strategic effectiveness of the organisation and there is possibility of it occurring.

h **Risk Mitigation** refers to actions that must be taken to lower the likelihood of the risk occurring and/or to minimize the impact if the risk did occur.

Related Ara Procedures	**Related Ara Policies**
• Council Health and Safety Charter • Hazard and Risk Management Procedure • Quality Assurance Framework	• CPP110 Legislative Compliance • CPP501 Health and Safety • CPP311 Treasury
Related Legislation or Other Documentation • Te Pūkenga Risk Management Framework 2022	**Related Standards**
References	
Notes	

2 Principles

2.1 Ara is committed to proactively and consistently managing risk with the objective of achieving maximum value from activities across the organisation to ensure we achieve our organisational goals and objectives laid out in Vision 2030 and associated strategic documents.

2.2 Ara seeks to maintain an open and receptive approach to solving risk problems across the organisation ensuring early identification and resolution.

2.3 The cycle of continuous improvement is embedded in risk management ensuring continuous review and improvement.

3 Associated Procedures for Ara Corporate Policy on: Risk Management

Contents:

3.1 Risk Assessment
3.2 Monitoring and Review
3.3 Review and Improve

3.1 Risk Assessment

To provide a structure for identifying, recording, and managing risks at Ara, a number of tools and guidelines have been designed.

a **Key Risk Register**

i The key risk register is designed to support managers as they identify a risk and have a need to assess the risk.

ii Risks will be mapped against the determined risk categories, with reference to Ara strategic plans and Vision 2030.

iii Faculties and Divisions maintain and manage Risks for their individual area by recording risks that are rated as minor or moderate on this one size fits all Risk Register.

iv The Risk Register "Headings" have pop-up descriptions to assist and support managers as they work through assessing an identified risk.

v The Key Risk Register template automatically calculates the overall Risk Rating in terms of the likelihood of it occurring and impact if it did.

b **Risk Management and Mitigation**

Ara has five main ways in which it can effectively apply a treatment to manage a risk.

i **Accept the risk** and make a conscious decision to not take any action.

ii **Reduce the risk** by taking action to lessen or minimise its likelihood or impact.

iii **Transfer the risk** to another individual or organisation, by, for example, outsourcing the activity.

iv **Finance (insure against)** the risk.

v **Eliminate the risk** by ceasing to perform the activity causing it.

Risk Mitigation Plans are put in place for all risks rated higher than moderate. The plans are developed by the Director accountable for the area the risk was identified in and monitored through regular reporting to TKM.

c **Risk Monitoring & Reporting**

i The Manager of Projects & Strategic Initiatives in alignment with the Director – Strategy, Planning, Performance is responsible for maintaining and monitoring the Risk Register and the Key Risks.

ii These risks are reviewed and reported quarterly to Audit and Risk Committee and the Ara Council on the status of those risks.

iii The register records description, background, indicators, all internal controls (key controls), further actions, risk ownership and links to strategic themes.

iv All actions are assigned action owners and agreed completion dates. The Risk Register is monitored by the Manager of Projects & Strategic Initiatives, who is responsible for this document and reporting exceptions to management. As part of this process, the Manager of Projects & Strategic Initiatives will liaise with the risk owners to –

- Request confirmation/ evidence to support the closure of completed actions.

- Request risk owners review controls to ensure they are current and are having the desired impact.
- Reassess the risk rating of risks following any changes in circumstances, such as extension/ completion of open risk mitigation plans.
- Obtain approval from the Risk Owner to support any changes in risk ratings i.e., changes in impact and/or likelihood.

v Risk ratings will be reviewed quarterly. Reviews will take into account actions delivered, processes embedded and any control remediation that has taken place. This will enable management to adjust the individual risk scores (either increase or decrease in rating), in light of changes to the overall risk environment within Ara.

vi Each Division and Faculty are responsible for recording risks as part of internal business planning and quality improvement processes. Risks identified, analysed, and assessed as having a significant to extreme impact on the organisation are escalated to a director to be analysed and assessed at TKM and a risk mitigation plan put in place where appropriate.

d **Guidelines for Risk Assessment**

The Risk Rating guidelines outline the steps required for risk assessment at Ara. The outcome (Risk Rating) at the end of the process will determine if the risk needs to be elevated to a Director. The guidelines are designed to support you as you complete the Risk Register. Once completed the risk will have been assessed and a rating applied.

i **Step 1:** A risk has been identified by a colleague and brought to the attention of a manager.

ii **Step 2:** Linking identified risks to objectives

The first step is to ensure that the identified risk is a risk to the achievement of the Ara goals and objectives by allocating a Risk Type, Risk Category, and mapping it to a Strategic Outcome. These have been defined in the Risk Register template as follows:

- **Risk Type**
  - Transformation
  - Business Controls
  - Learner Outcomes
  - Colleague Capability
- **Risk Category**
  - Attraction and retention of learners
  - Strategic
  - Financial
  - Project/Asset Management
  - Programme delivery
  - Technology
  - Compliance
  - Recruitment and retention of colleagues
  - Business Continuity

- **Strategic Outcomes**
    - Personalised, flexible learner journey to achievement
    - Responsive and agile portfolio and delivery
    - High performing organisation

iii **Step 3:** Linking identified risks to objectives

The third step is to determine the impact the risk would have. Five types of impact have been identified, as well as five levels for rating the impact.

- **Type of Impact**
    - Reputational
    - Strategic
    - Operational
    - Compliance
    - Financial

- **Type of Impact**

  There are five levels of impact rating ranging from Minor to Extreme. (Note: the identified risk should be assessed against each of them.)

Risk Impact Criteria

	*Note: (The Type of **impact** must also be considered against each risk e.g., Reputational, Strategic, Operational, Compliance, Financial)*			
Rating	**Level of Impact**	**Example impacts**	**Level of Interest**	**$ Value**
1	**Minor**	Minor reduction of learners **Undesired loss of colleague** Minor impact on organisational strategic goals and operational activities	Minimal public or local interest Event that involves Level 400 Manager management time	Under $1m in any 12-month period
2	**Moderate**	Moderate reduction of learners **Undesired loss of colleagues** Moderate impact on organisational strategic goals and operational activities	Moderate public or local interest Event that involves Level 300 Manager management time	$1-2m in any 12-month period.
3	**Significant**	Undesirable reduction of colleagues and learners in a course Undesired loss of an academic course Significant impact on organisational strategic goals and operational activities	Significant public or local interest Event that involves Level 200 Manager management time	$2-3m in any 12-month period.
4	**Major**	Undesirable reduction of colleagues and learners in a programme Undesired loss of an academic programme Organisational strategic goals and operational activities are impacted such that there is an undesired loss of colleagues and curtailment of activities	Major public or media attention Event that involves CE management time	$3-5m in any 12-month period.

	*Note: (The Type of **impact** must also be considered against each risk e.g., Reputational, Strategic, Operational, Compliance, Financial)*			
Rating	**Level of Impact**	**Example impacts**	**Level of Interest**	**$ Value**
5	**Extreme**	Undesirable reduction of colleagues and learners in a Faculty/Institution Undesired loss of a Faculty/Institution Organisational strategic goals and operational activities are impacted such that there is an undesired loss of colleagues and closure of Faculty/Institution	Serious or sustained public and media attention Event that involves the Council management time	Greater than $5M in any 12-month period

iv **Step 4:** Determine the likelihood of the risk occurring.

The second rubric on which the risk is assessed is the likelihood of the risk occurring. The following definitions of likelihood are used:

Rating	**%**	**Likelihood Criteria (within 12-24 months)**
1	0 - 10	Highly unlikely to occur
2	10 - 25	Possibility of occurrence
3	25 - 75	Real possibility of occurrence
4	75 - 90	Likely to occur
5	90 - 100	Almost certain to occur

v **Step 5:** Multiply the Impact and Likelihood Ratings to produce the risk rating

The next step is to multiply Impact by Likelihood to produce the overall risk rating.

Impact x Likelihood = Overall Risk Rating

Given that we have used a five-scale rating for Impact and Likelihood, this will result in a number between 1 and 25. The following impact ratings were used to categorise the overall risk:

Impact						
	5	5	10	15	20	30
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Likelihood				

Overall Risk Ratings	
1, 2, 3	Minor
4, 5, 6	Moderate
8,9,10,12	Significant
15,16	Major
20, 25	Extreme

vi **Step 6:** Next steps

The risk rating automatically calculates on the register.

The rating applied determines the next steps – see below.

Overall Risk Rating		Step 1	Step 2	Step 3	Step 4
1, 2, 3	Minor	Manager adds it to the Division/Facultyregister	Risk Treatment applied; Accepted, Reduced, Transferred, Eliminated, Removed	Monitored & reviewed by Manager. Ownership with Manager. An action tracking column is maintained in the risk register, which allows Ara to identify ownership	Monitoring occurs through regular reporting to TKM, the CE and Audit & Risk Committee
4, 5, 6	Moderate				
8, 9, 10, 12	Significant	Escalated to the Chief Executive. The Ara Council is informed.	Risk Assessed at TKM TKM informs the Chief Executive, Director - Strategy, Planning, Performance via the Manager of Projects & Strategic Initiatives updates Key Risk Register	Risk Mitigation Plan put in place by accountable Director. Council informed.	Monitoring occurs though regular reporting to TKM, the CE and Audit & Risk Committee
15, 16	Major				
20, 25	Extreme				

vii Key points to note when applying risk ratings –

- For the Risk Ratings, when assessing a general risk (such as, "Critical ICT system failure resulting in loss of critical data"), the impact and likelihood of the event will vary widely, depending on the nature of the event.
- It is not practical to attempt to define all ICT system failure events that may lead to loss of data since many will not be of sufficient significance to warrant this effort.
- Therefore, the approach is to apply the lowest Impact and Likelihood Ratings that will still result in the risk being rated as Significant.

  Either:

  "Impact = 3, Likelihood = 3, Risk Rating = 9" OR
  "Impact = 2, Likelihood = 4, Risk Rating = 8" OR
  "Impact = 4, Likelihood = 2, Risk Rating = 8"
- Management determines what type of events fall into which category, based on the Impact and Likelihood definitions.

3.2 Monitoring and Review

a **Process**

i Operations maintains a Risk Register that identifies and registers Key Risks. The register is informed by risks identified at department and division level across the organisation.

b **Reporting**

i The Key Risk register is formally reported to TKM, Audit & Risk Committee, and the Council as laid out in the Schedule below.

ii New risks as well as any change to risk assessments are reported monthly to TKM. **Note:** Risks which are assessed as Significant, Major, or Extreme are referred

immediately to TKM and the Chief Executive for assessment and mitigation, and the Council informed

Proposed Key Risk Register Review & Reporting Schedule				
Month	Operations Review	TKM Risk Report	ARC Risk Register Report	Council Risk Register Report
January	✓	Review		
February	✓	TKM		
March	✓	Review	ARC	
April	✓	Review		Council
May	✓	TKM		
June	✓	Review	ARC	
July	✓	Review	ARC	Council
August	✓	Review		
September	✓	TKM		
October	✓	Review	ARC	
November	✓	Review		Council
December	✓			

3.3 Review and Improve

a The Ara risk management processes will be reviewed in line with the principles of continuous improvement. Ara will take a proactive approach to recognising and assessing key risk indicators.

b To provide an early signal of increased risk exposure to the organisation, review of the 'key risk Indicators' will occur at TKM and Academic Committee meetings, as well as at Management meetings across the organisation, namely Faculty Leadership Team, Ākonga Success, Corporate Services, People and Culture and Treaty Partnerships.

c The Key Risk Register Indicators will be tabled at management meetings with a short purpose statement to encourage a conversation around new risks, and a corresponding review of the Key Risk Register Controls to ensure they are adequate to manage the risk.

Key Risk Indicators
• Insights from TEC through the relationship with Ara. • Failure of another ITP. • Learner/colleague feedback and communication. • Negative media coverage on the transformation and change programme and impact on local communities.
• Stakeholder feedback that we are not being responsive to their needs. • Declining international applications by market. • Failure to renew collaborative agreements. • Non-compliance with the agreements. • Drop in stakeholder survey results. • Failure to reach agreement. • Lack of clarity of party responsibilities. • Limited work integration opportunities impacting on our ability to place learners.
• EPIs • Dropping of enrolments. • Immigration policy change monitoring of projects expected benefits not reached. • Staffing viability.

• Benefits realisation.
• Pattern of applications and enrolments, e.g., low enrolments in some regions and programmes. • Conversion of applications into enrolments. • Reduced revenue. • Withdrawal trends. • Priority group participation targets. • Student satisfaction surveys.
• Inconsistent / variable data. • Unanticipated performance outcomes. • Reliance on external data.
• Health and Safety incidents are not reported (low near missed and incident reporting). • High number of sick days. • High turnover of colleagues.
• Usage of professional development budget. • Percentage of staff with Professional Development plans in place. • student survey results in respect of tutors etc.
• Learner or colleague health and safety notifiable incident. • Learner or colleague complaints. • Union tensions - interaction with union colleagues before Ara colleagues. • Programmes closed due to minimum numbers of students not being met. • Comply With non-compliance detection increases or is consistently flagged. • Media coverage.
• Employer/ Voice survey. • Colleague survey. • Learner survey. • Employment Outcomes of Tertiary Education (government data). • Feedback from Industry Advisory Groups. • External Evaluation Review report.
• Increased number of minor incidents. • Connectivity issues. • Helpdesk call logging. • Service level agreements in place. • Testing and monitoring environment.
• Fire drill response. • Facility non-compliance. • Maintenance programmes.

Schedule 1: Roles and Responsibilities

Specific roles and responsibilities for risk management at Ara are as follows –

All Colleagues	• Responsibility for risk management rests with every colleague. All colleagues (where appropriate) are required to identify and report new risks or a change in the status of existing risks in a timely manner to their line manager.
Faculty Deans, Portfolio Managers, Operations Managers	• Identify and analyse strategic, operational and project risks within Faculties and Divisions • Elevate significant risks to a Director for consideration at TKM. • Record and monitor minor to moderate risks on a risk register, determining whether to minimise the risk or accept it. • Identify and report new risks or the change in the status of existing risks in a timely manner to their line manager.
Te Kāhui Manukura (TKM)	• TKM Directors are accountable for risk management within their portfolios. • Identify, analyse, monitor and report on Key risks, strategic, operational and project risks. • Risk owners of Key Risks within the organisation. • Risk assessment, management, monitoring and reporting to the Director - Strategy, Planning, Performance for all risks. • Delivery of all relevant risk mitigation plans which contribute towards the management of risk within Ara. • Approval of the Risk Management and Legislative Compliance Frameworks.
Director – Strategy, Planning, Performance, Manager of Projects & Strategic Initiatives	• Delegated responsibility for management of the risk policy, monitoring and maintenance of the risk register, and regular reporting to Audit & Risk committee and the Council on the status of those risks. • Maintenance and dissemination of the Risk Management Procedures and Diagram. • Management oversight of risk management and legal compliance. • Regular maintenance and review of the risk register ensuring mechanisms are in place for effective risk management.
Chief Executive	• Management responsibility for risk management and legal compliance. • The Chief Executive is responsible for overall risk management.
Audit & Risk Committee	• Maintain overview of financial risk and legal compliance at Governance level. • Review the risk management framework ensuring it meets requirements and includes policies and processes to effectively mitigate/manage risks. • Review risk reporting to the Council, including the annual review of the risk register.