RISK MANAGEMENT FRAMEWORK

INTRODUCTION

Risk Management is an enabling function that adds value to the activities of the organisation and increases the probability of success in achieving our strategic objectives. It's about managing uncertainty and creating an environment where surprises are minimised.

This document defines the practices adopted by the University to identify risk, in order to reduce potential negative impacts, and improve the likelihood of beneficial outcomes.

The benefits of creating a practical Risk Management Framework that can be applied across all part of the University include:

- A consistent, structured approach to identifying and managing risk
- Supports the achievement of the University's strategic and operational goals by managing risks that may otherwise impede success
- Encourages an open and transparent culture where risk discussion and awareness are supported
- Better decision making practices that support risk informed choices, prioritize actions and distinguish between alternative courses of action
- Encourages an understanding of the risk environment within which the University operates
- Provides assurance to the Vice Chancellor and Council that critical risks are being identified and managed effectively.

The management of risk happens every day across all parts of the University, in many different ways. The following examples demonstrate some of the existing processes in place for how Massey mitigates risk:

Health and Safety at Work: To ensure the safety and wellness of workers at Massey, there are a number of processes established to minimise workplace harm including but not limited to: hazard identification, induction, health monitoring, training and development, incident reporting and remediation.

Code of Conduct: The University has both Staff and Student Codes of Conduct which define the required behaviours of staff and students of Massey University.

Research: Codes of Ethics and Committees to ensure application and compliance to these Codes, supervision, peer reviews, organisation structures and specialist appointments such as designated lab and facility managers, physical audits.

Physical Security: Dedicated security resourcing to ensure the safety of the University community and facilities.

Internal Audit: Provides assessment and review of key internal controls, and the control environment.

Academic Quality: Quality of the University's academic portfolio is ensured through the CUAP accreditation process, and peer review processes.

Business Continuity and emergency management: Policy and Framework govern the operational structures, activities and arrangements for emergency management in line with best practice Reduction, Readiness, Response & Recovery processes.

The framework is aligned to our business outcomes and the strategies designed to achieve these outcomes.

The process used to identify and manage risk at Massey University aligns with the AS/NZS ISO 31000:2009 Risk Management Standard. This Framework should be read in conjunction with the University's Risk Management Policy.

AN EFFECTIVE ENTERPRISE RISK MANAGEMENT SYSTEM

For risk management to be effective, it is important that University staff and stakeholders have a shared understanding of what an effective system for risk management looks like, and how we will achieve this. The ISO 31000:2009 Standard recommends organisations adopt the following principles:

Guiding Principles

The following ten principles[1] are the foundation of the Risk Management Framework and are the key drivers to ensuring a consistent, fit-for-purpose approach to managing risk at the University.

1. **Risk management adds value** by contributing to achievement of objectives and improving performance, for example via legislative and regulatory compliance, use of reliable and accurate information for decision-making, effective project management, operational efficiency and robust governance.

2. **Risk Management is an integral part of organisational processes.** Risk Management is part of the responsibilities of management and an integral part of University processes, including strategic planning and all project and change management processes and decision making.

3. **Risk Management is part of decision making.** Risk Management helps decision makers make informed choices, prioritize actions and distinguish among alternative courses of action.

4. **Risk management explicitly addresses uncertainty** by identifying and describing the nature and source of that uncertainty.

5. **Risk practices are systematic and structured and timely,** ensuring consistent, comparable and reliable results which contribute to efficiency.

6. **Risk management is based on the best available information** including historical data, experience, stakeholder feedback, observation, evidence, forecasts, and expert judgement.

7. **Risk management is tailored** to align with the University's external and internal context and risk profile.

8. **Risk management practices are transparent and inclusive,** ensuring appropriate and timely involvement of stakeholders and decision makers at all levels of the organisation. Involvement also allows stakeholders to be properly represented and to have their views taken into account.

9. **Risk is dynamic, iterative and responsive to change.** Effective risk management should always consider the internal and external operating context. As external and internal events occur, context and knowledge change, monitoring and review of risk take place, new risks emerge, some change and others disappear.

10. **Risk management facilitates continual improvement of the organisation** by implementing risk mitigations which improve the University's probability of achieving its goals, and by building capability to recognise and reduce or take managed risk.

The Risk Management Office will periodically review and confirm that each principle continues to be satisfied and is tailored to meet the needs of the University.

---

[1] AS/NZS ISO 31000:2009 Australian/New Zealand Standard: Risk management – Principles and guidelines.

RISK GOVERNANCE

Mandate and Commitment

The mandate for risk management comes from the University Council and Senior Leadership Team (SLT). The continued engagement and support of these groups is critically important – without it, risk management fails. These governance groups understand this and are committed to ensuring sustainable and effective risk management within the University. This commitment must be mirrored by management and staff at all levels.

The University Council and SLT lead this commitment by:

- endorsing and implementing the Risk Management Framework, and Policy and ensuring that these are updated to remain relevant

- understanding the value added by risk management and communicating this to staff and stakeholders

- aligning risk management activities with the achievement of organisational objectives

- ensuring legislative and regulatory compliance

- assigning accountabilities and responsibilities for risk management at appropriate levels within the organisation

- ensuring independence of the Risk and Assurance team such that risks can be raised to the highest level without fear of punitive outcome

- creating and supporting an organisational culture which encourages transparent identification and open discussion of risks

- monitoring the effectiveness of the risk management system and ensuring actions are taken to continually improve it.

Roles and Responsibilities

Effective Risk Management requires clear lines of accountability. The University maintains several committee structures, to co-ordinate some aspects of risk management. These committees provide instruction and guidance and do not absolve the line managers of the need to discharge their responsibilities in relation to managing risk.

Massey University Council: The University Council oversees the University's operations, establishing both the strategic direction and financial performance targets for management and monitoring the achievement of these objectives. The composition and duties of Council are set down in legislation.

Audit and Risk Committee: The Audit and Risk Committee of Council assists the Council in discharging its responsibilities relative to financial reporting, risk management and regulatory conformance. In respect of risk management, the Committee is responsible for approving the Risk Management Framework, monitoring risk assessments and internal controls instituted, and to approve or recommend approval of risk related policies.

Senior Leadership Team (SLT) and Risk Management Committee: SLT have responsibility for overseeing key risk management controls, including but not limited to financial and management accounting, property, insurance purchasing, contractual liabilities, business continuity, people related, and other operational risk controls, and assessment of strategic risk within their areas of responsibility. The Risk Management Committee supports SLT as the key advocate for risk management at Massey and has specific risk management responsibilities.

Accountability for Risk Management

	Responsibility	Accountability
Risk Owner	Overall coordination of the management of the risk, including: Ensuring controls are effective, monitoring the completion/implementation of treatments; monitoring the environment; providing updates for University risk reporting.	Effective oversight and management of the risk. Communicating risk status when risk exceeds tolerability and, escalating when necessary.
Risk Lead	Maintain oversight of risks identified within their organisational area, in consultation with the Risk Owner. Providing status updates on risks and controls under the ownership of their Risk Owner.	Provide status updates on risks, treatments and controls within their area of responsibility, on behalf and in consultation with the Risk Owner.
Control/ Treatment Owner	Ensuring the control is effective through: ongoing operation and improvement; maintaining up-to-date assessment of control effectiveness. Implementation/completion of treatment; ensuring appropriate ownership once treatment is complete and in place as a control.	Effective oversight and maintenance of the control. Design and Implementation of the treatment to agreed timeframes and quality.
Director Risk and Assurance	Maintain oversight of University risks, controls and treatments: Reporting of University risks. Facilitate the risk management process. Reporting on any emerging risk issues. Monitoring internal and external environment in conjuncti0n with each portfolio area.	Maintain oversight of University risks. Report risks and risk issues to senior management and Council.

INTEGRATION INTO ORGANISATIONAL PROCESSES

Risk management should be embedded with University systems and processes to ensure that it is part of everyday decision making. In particular risk management must be embedded in the following key processes:

Annual planning and budgeting processes: Within each portfolio area, risk identification should occur as part of the annual planning cycle to inform planning and budgeting for the following year. Costs of implementing the annual plans, including consideration of costs associated to controls or treatments required need to be incorporated into the budgeting process.

Project and programme management: As part of good project management practice, risks are actively identified, managed, escalated and reported throughout the lifetime of the project.

Development and review of University policies and procedures: University policies and procedures specify the approach and expected actions required to manage a variety of risks, including those associated with legislative compliance, academic management, quality and equivalence, people management, finance and asset management.

Procurement and asset management: Risk management must be factored into decision making for significant procurement and asset management related processes.

ALIGNMENT OF RISK TO STRATEGIC OBJECTIVES

The AS/NZS ISO 31000:2009 Risk Management Standard defines risk as '*the effect of uncertainty on objectives*'.

The University is exposed to a diverse range of internal and external factors and influences that make it uncertain whether, when and the extent to which our objectives will be achieved.

The objectives referred to are expressed in the Standard as '*the overarching outcomes that the organisation is seeking. These are the highest expression of intent and purpose, and typically reflect its explicit and implicit goals, values and imperatives or relevant enabling legislation.*'[2]

Massey University articulates its strategic intent and purpose through its Investment Plan which is in turn informed by the following:

- Shaping the nation and taking the best to the world – The Road to 2025
- The Tertiary Education Strategy 2014-2019; and
- The letter of expectation prepared by the Tertiary Education Commission (TEC) for Massey University.

At a high level we can categorise the risks that Massey is exposed to as strategic or operational risks. All risks are managed within the same framework, as inadequately managed operational risks can escalate to become strategic risks.

Strategic risk

Strategic risks are risks that affect or are created by the University's strategy and strategic objectives, as defined in the Road to 2025.

Operational risk

Operational risks are events that will affect the University's ability to execute its strategic plan, and may arise from inadequate or failed internal processes (including people processes) and systems, or from external events that impact on the operations of the University. Types of operational risk may be broken down further into areas such as:

Project risk

Project risk may be defined as an uncertain event or condition that, if it occurs, has a positive or negative effect on one or more project objectives such as scope, schedule, cost, or quality.[3]

Compliance risk

Risk resulting from a failure to comply with laws, regulations, code of conduct, and accepted standards of best/good practice.

Health and Safety risk

Risks to people affected by the conduct of work being undertaken at the University.

---

[2] SA/SNZ HB 1436:2013: Australian/New Zealand Handbook Risk Management guidelines – Companion to AS/NZS ISO 31000:2009
[3] 5th Edition of the PMBOK® Guide

RISK ASSESSMENT CRITERIA

The following risk assessment criteria will be used for risk analysis at Massey University. Risk analysis involves consideration of the sources of risk, the controls in place (and their actual effect), the consequences and the likelihood of those consequences being realised.

Likelihood assessment

Rating	Likelihood criteria (12-36 months or within project lifetime)
Almost Certain	Is expected to occur Definite probability Without additional controls the event is expected to occur in most circumstances
Likely	Will probably occur in most circumstances With existing controls operating this event will probably still occur with some certainty
Possible	Could occur at sometime The event has occurred in different industries with similar levels of controls and assurance in place
Unlikely	Not expected to occur The event hasn't occurred, but it could occur in some circumstances
Rare	Exceptional circumstances only Improbable A small chance of event occurring that would be caused by conditions and/or events not previously seen.

Assessment of effectiveness of controls

The following control assessment criteria should be used to assess the overall effectiveness of the controls in place that are mitigating the risk. Note that the controls identified may not always exert the intended or assumed modifying effect, or are not yet at a point where they are fully operational or effective.

Rating	Level of protection/mitigation
Excellent	Controls practices are fully embedded in business processes. Continuous improvement programmes are operating to improve efficiency and effectiveness of controls.
Good	Optimal levels of Controls are in operation at all times. Control practices are embedded in business processes.
Sufficient	Sufficient Controls are in place for day-to-day operations but control practices are not fully embedded in business as usual processes yet.
Insufficient	Insufficient Controls are in operation (i.e. yet to be implemented, not implemented effectively and/or additional Controls are needed). Control breaches are common.
Non-existent	No identified or planned Controls.

Consequence Assessment

When determining consequence level, to safeguard from the unnecessary application of treatments and costs, the consequence rating applied should be the most plausible, not the most extreme worst-case scenario.

The following pages detail the consequence assessment criteria for organisational and project specific risks.

UNIVERSITY CONSEQUENCE MATRIX

CONSEQUENCE ASSESSMENT MATRIX

	MINOR	MODERATE	SIGNIFICANT	MAJOR	SEVERE
HEALTH AND SAFETY	Would cause minor illness and injuries that are able to be treated at the site with no long-term effects or days lost.	Would cause minor illness and injury that require medical attention off-site with no long-term effects and some days lost.	Would cause possible hospitalisation(s) and numerous days lost with no long-term effects.	Single death &/or long-term illness or multiple serious injuries.	Would cause fatality (ies) or permanent disability or ill-health.
COMPLIANCE AND LEGAL	Contract: Minor contractual breach, sanction from other party with potential small compensation. Regulatory. Minor non-compliance able to be remedied without penalty or notification.	Contract: Potential for dispute, mediation likely and/or with potential small compensation Regulatory: Mandatory reporting of non-compliance,	Contract: Material breach of contractual obligation, potential litigation or large settlement Regulatory : Investigation by regulator	Contract: Single Litigation. Regulatory: Sanction or prosecution by regulator	Contract: Multiple Litigations. Regulatory : Major compliance breach, or multiple breaches that result in prosecution or maximum penalty or sanction by regulator
REPUTATION	External Reputation not affected. No effort or expense required to recover.	Media attention no more than 1 day. Negative association with Massey brand (stakeholder).	Regional media attention 1-3 days, little effort or expense required to recover. Marginal drop in international ranking. Potential medium term impacts to being seen as provider or partner of choice.	Nationwide media attention, greater than 2 days. National headlines, variety of media. Requires effort or expense to recover and mitigate. Significant drop in international ranking. Significant impacts to attractiveness as provider or partner of choice	Sustained media attention, including international exposure. Significant damage to Massey brand, requiring urgent effort or expense to recover. Involves unplanned VC/Council time to address. Serious and sustained impacts to attractiveness as provider or partner of choice.
FINANCIAL	Financial impact $0-150k OPEX, within 12 month period.	Financial impact $150- $500k OPEX, within 12 month period. Budget impacts to individual unit, short term impact to operations.	Financial impact $500k-$1M OPEX, within 12 month period. Budget impacts across multiple portfolios, affects operations and performance.	Financial impact $1M-$5M OPEX, within 12 month period. Budget issues affect 1-3yr capital plans. Cost management measures required across all portfolios.	Financial impact >$5M OPEX within 12 month period. Budgetary impacts across MU, affecting long term capital plan. Budget surplus at risk, extraordinary measures required.
PERFORMANCE AND CAPABILITY	No impact on quality of services delivered. Negligible performance impact.	Minor impact on the delivery or quality of services. Substandard quality of delivery or operation of core service or activity.	Some impact on the delivery or quality of services. Workarounds required to maintain operation of core service or activity.	Considerable impact on the delivery or quality of services. Core service is partially functional. Impedes or significantly delays achievement of key strategic objective, significant workarounds and impact to BAU.	Major impact on the delivery or quality of service or operation. Sustained Inability to deliver core service (i.e. enrolments). Prevents achievement of key strategic objective Major impact to College or viability of multiple programmes.

PROJECT CONSEQUENCE MATRIX

PROJECT CONSEQUENCE ASSESSMENT MATRIX					
	MINOR	**MODERATE**	**SIGNIFICANT**	**MAJOR**	**SEVERE**
TIME	Insignificant delays, minimal impact on project timeline.	Non-critical tasks are not completed on time.	Critical tasks not completed on time. Likely downstream impacts to project timelines and delivery dates. Timeline is behind schedule.	Key milestones are missed and significant delay to the project delivery date. Timeline is behind schedule with a key date or critical missed.	Severe impact to schedule, and/or missed critical fixed delivery dates. Significantly behind schedule with multiple key dates/milestones have been missed.
COST	Financial loss or budget overrun the lesser of 10% or $250k of phase/project.	Financial loss or budget overrun the lesser of 10-15% or $500k of phase/project.	Financial loss or budget overrun the lesser of 15-20% or $1M of phase/project. The value or cumulative value of change requests and/or variations exceeds 10% of budgeted project contingency.	Financial loss or budget overrun the lesser of 25% or $1.5M of phase/project. The value or cumulative value, of change requests and/or variations exceeds 25% of the budgeted project contingency	Financial loss or budget overrun above 33% or $2M of phase/project. The value/ cumulative value, of change requests and/or variations exceeds 50% of the budgeted project contingency.
QUALITY	Insignificant impact on overall quality of product or service. No action required to achieve planned business outcomes.	Minor impact to the quality of the output, remedied without additional cost. Limited/few hazards identified or created	Moderate impact on the quality of output Additional activities or cost required to remedy quality issues Failure to meet legal or regulatory requirements, and/or potential litigation or penalty Notifiable incident.	Considerable impact on quality of output. Requires significant additional effort either during or post project to achieve acceptable levels of performance. Serious harm injury. Non-compliance with legal/regulatory requirements - potential litigation or penalty	Severe impacts on the quality of the product or service delivered. Without remediation the product is considered to be unstable and not fit for production use. Death of an individual.
SCOPE ACTIVITIES OUTPUT	No impact on project deliverables. All intended outcomes are achievable.	Minor impact on deliverables, and 'nice to have' functionality No impact to intended outcomes some workarounds in place. Some adverse public reaction or cultural impact.	Moderate impact to deliverables - 'could have' functionality not delivered. Reputation damage or moderate cultural impact Loss of business efficiency	Major impact to deliverables with 1 or 2 'must have' features not delivered. Requires significant workarounds or inability to meet needs. Significant loss of business efficiency Numerous and/or major hazards are identified	Severe impact to project deliverables with more than 2 'must have' features not being delivered. Product or service does not deliver the key intended outcomes for the business. Sustained and significant loss of business efficiency
RESOURCES	Insignificant impact to resourcing, manageable within the overall baseline for project delivery.	Minor impact to approved project resourcing requiring additional resource and increase in overall effort.	Moderate impact to approved project resourcing requiring additional short-term resource and increase in overall effort. Insufficient adequately skilled dedicated project resources	Major impact to approved project resourcing requiring multiple additional resources with an overall increase of effort Insufficient adequately skilled dedicated project resources	Severe impact to approved project resources requiring significantly more resources for an extended period of time to achieve the agreed project outcomes.
BENEFITS AND OUTCOMES	No impact in overall ability to realise planned benefits. Additional effort or workarounds required to achieve the intended benefits.	Minor impact in ability to realise planned benefits. Some of the less fundamental benefits may not be fully realised.	Moderate impact on ability to realise benefits. Additional effort and manual tasks required to achieve benefits. Minor impact to intended outcomes. Reduced likelihood of attaining primary objectives.	Major impact on ability to realise benefits. Significant additional work required to achieve benefits. Noticeable impact to intended outcomes. Incident/events/variations greatly reduce attainment of primary objectives.	Critical benefits will not be realised by the project. Significantly reduced probability of attaining primary objectives . Variation and scope changes significantly erode expected benefits.

RISK TOLERANCE AND ACCEPTABILITY

This matrix is used to determine risk rating by combining the consequence and likelihood levels. The assessment is used to determine the severity of the risk and identify those which are unacceptable to the University and require management attention and further treatment. It also forms the basis of ongoing monitoring.

Likelihood	Consequence				
	Minor	Moderate	Significant	Major	Severe
Almost Certain	Low	Medium	High	Very High	Very High
Likely	Low	Medium	High	Very High	Very High
Possible	Low	Medium	Medium	High	Very High
Unlikely	Low	Low	Medium	Medium	High
Rare	Low	Low	Low	Medium	Medium

The following table is to be used as a guide to determine whether a risk requires additional treatment. If the assessed risk rating is above the tolerable level for that impact area, then treatment is required that will either reduce the likelihood of the event occurring, or the impact should it be realised. If the risk rating is at or below the target level as indicated then the risk may be accepted. (Please note that project risk tolerance and acceptability should be specified as part of a risk and issues management plan for the project.)

Impact area	What level of risk are we willing to accept in the pursuit of our objectives?			
	Low	Medium	High	Very High
Health and Safety		♦		
Compliance/Legal		♦		
Performance & Capability		♦		
Financial		♦		
Reputation		♦		

If there is no further treatment that can be applied to mitigate the risk (and reduce either the likelihood or the consequence), or the cost of applying the required treatment outweighs the impact or the benefit, then formal acceptance of the risk may be provided by the following:

Impact area	Authority for acceptance/retention of risk outside risk tolerance level			
	Low	Medium	High	Very High
Health and Safety	X	X	SLT or VC	COUNCIL
Compliance/Legal	X	X	SLT or VC	COUNCIL
Performance & Capability	X	X	SLT or VC	VC/COUNCIL
Financial	X	X	SLT or VC	VC/COUNCIL
Reputation	X	X	SLT or VC	COUNCIL

TREATING AND ACCEPTING RISKS

Risk treatment options should be based on cost benefit analysis of outcomes, i.e. does the cost of applying the required treatment or control outweigh the impact or the benefit? Treatments are essentially based on one (or a mixture) of the following options.

Avoid: Treating the risk by avoiding the event that would lead to the risk occurring. For example: not entering a new market, not pursuing an opportunity.

Mitigate: Develop a plan to reduce the likelihood and/or consequence. This involves taking pre-emptive action along the lines of:

- Identify the range of treatment options
- Assess the options (timely, cost effective, what resources are required, is it feasible)
- Select the most effective options(s), assign each a treatment owner
- Develop the plan, incorporate into existing plans (annual plan, project plan)
- Develop contingency responses (BCP, DRP) if necessary

Retain: Accept the likelihood and consequence of the risk occurring.

Transfer the risk in part or in full (i.e. insurance, contractual agreements)

Accept the risk (i.e. if the benefit outweighs the cost)

Where the assessed risk rating is above the tolerable level for that impact area, then the implementation of the treatment or mitigation should be monitored to ensure it has the intended effect of reducing the risk down to a tolerable level.

RISK MONITORING AND REPORTING

Portfolio

Assigned risk owners will review their risk registers at least 6 monthly and consider any changes in their respective areas, including: maturity and effectiveness of controls or treatments being applied to mitigate existing risks, and; identifying any new risks which are emerging as a result from changes in the internal or external environments.

Identifying and managing risk is a key part of annual planning. These processes define plans and allocate resources to achieve certain objectives. An integral part of planning is to identify anything that might threaten the achievement of those objectives.

The Risk Management Office will support risk owners in this process, and undertake an annual review of identified risks and controls, encompassing strategic, environmental, and annual planning changes.

Quarterly Risk Reporting

Risk reports are prepared quarterly for the Senior Leadership Team and the Audit and Risk Committee, detailing:

- Those risks which are outside the acceptable tolerance levels
- Details of any escalating risks, and emerging risk issues considered during the reporting period
- Significant project risks

KEY RISK DEFINITIONS

The following key risk definitions are taken from the AS/NZ ISO31000:2009 Risk Management Standard:

DEFINTIONS	
Risk	Effect of uncertainty on objectives
Risk Management	Coordinated activities to direct and control an organisation with regard to risk
Risk Owner	Person or entity with the accountability and authority to manage a risk
Control	A measure that is modifying risk Note 1: includes any process, device, practice or other actions that modify risk Note 2: May not always exert the intended or assumed modifying effect
Treatment	Process used to modify risk Note 1: can involve avoiding the risk, accepting/retaining the risk, removing the source of risk, changing the likelihood or consequence, sharing risk Note 2: May also ne known as risk mitigation
External context	External environment in which the organisation seeks to achieve its objectives. Note: can include the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local.
Internal context	Internal environment within which the organisation seeks to achieve its objectives. Note: can include governance, organisational structure, roles and accountabilities, policies, objectives and strategies, information systems and decision making processes, culture and capabilities.
Consequence	Outcome of an event affecting objectives Note 1: An event can have a range of consequences Note 2: A consequence can be certain or uncertain and can have positive or negative effects on objectives
Likelihood	Chance of something happening
Risk source	Element which alone or in combination has the intrinsic potential to give rise to risk.