The Australian Centre for Excellence in Antarctic Science (ACEAS)

Risk Analysis and Management Plan

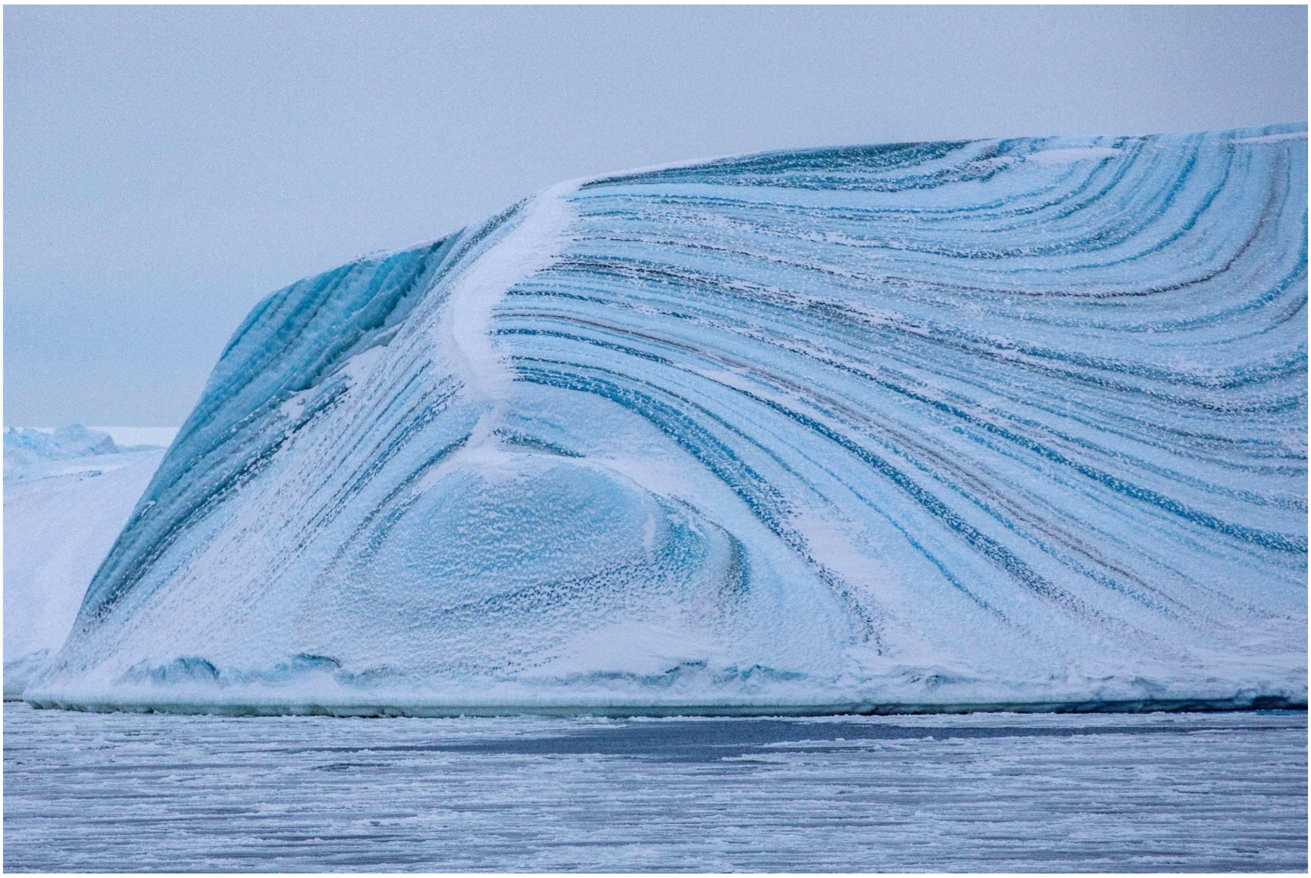

Image Credit: Pete Harmsen / AAD

Table of Contents

1. RISK ANALYSIS AND MANAGEMENT PLAN 3

1.1. Purpose and Scope 3
1.2. Risk Management Framework and Approach 3
1.3. Risk Governance, Roles and Responsibilities 3
1.4. Key Risk Categories 3
1.5. Risk Register Summary 4
1.6. Monitoring, Review and Reporting 4
1.7. Continuous Improvement 4

2. RISK REGISTER 5

APPENDIX I: RISK ASSESSMENT TOOL RUBRIC 8

1. Risk Analysis and Management Plan

1.1. Purpose and Scope

This Risk Management Plan identifies, assesses, and outlines strategies to manage risks that may affect the successful delivery of the project. The plan supports compliance with the Advancing Australia's National Interests in Antarctica Grant Opportunity Guidelines and the associated Commonwealth Standard Grant Agreement, and demonstrates the project's capacity to deliver agreed activities, milestones, data outputs, and publications on time and within budget.

such as

1.2. Risk Management Framework and Approach

Risk management for this project follows a structured, qualitative approach consistent with widely accepted good practice. Risks are identified at the project, work package, and delivery levels and are assessed according to their likelihood and consequence should they occur. Appropriate mitigation strategies and contingency measures are then applied.

Risks are reviewed regularly throughout the project lifecycle and updated as required in response to emerging issues, changes in project scope, or variations to the grant agreement.

1.3. Risk Governance, Roles and Responsibilities

Overall responsibility for project risk rests with the Project Director on behalf of the University of Tasmania. Specific risks are managed by designated risk owners, including Work Package Leads and institutional partners, with escalation pathways through ACEAS governance structures, including the Project Management Committee.

Financial, data governance, work health and safety, and compliance risks are managed in accordance with University of Tasmania policies and procedures and the obligations set out in the grant agreement.

The project is subject to audit, inspection, and record-keeping requirements under the grant agreement, with records retained and made available to the Commonwealth as required.

1.4. Key Risk Categories

The primary risk categories for the project include:

- Scientific and technical risks
- Schedule and delivery risks
- Financial and budget compliance risks
- Data governance and Antarctic Data Policy compliance risks
- Consortium and partner risks
- Personnel capability and continuity risks
- Work health and safety risks

-
- Legal, probity, and integrity risks
- External and force majeure risks

1.5. Risk Register Summary

A detailed risk register is maintained for the project. Each risk is assigned a likelihood, consequence, overall rating, mitigation strategy, residual risk assessment, and a named risk owner. Early warning indicators are used to identify issues at an early stage and enable proactive management.

Typical mitigation strategies include early data audits, staged milestone delivery, dedicated data stewardship, structured financial monitoring, fraud prevention controls embedded in University of Tasmania financial systems, and the use of partner university agreements to manage partner responsibilities. Any suspected fraud, misuse of grant funds, or serious non-compliance will be reported to the Commonwealth in accordance with contractual and legislative obligations.

Data risks are managed with the understanding that required datasets will be provided to the Commonwealth and made available for reuse in accordance with the grant agreement, while intellectual property ownership is retained by the grantee.

1.6. Monitoring, Review and Reporting

Risks are reviewed at regular project meetings and formally reassessed at key milestones. Material risks that may affect project outcomes, timing, or compliance are escalated to the appropriate governance level.

The project will provide prompt written notification to the Commonwealth of any event or risk that is reasonably likely to adversely affect project delivery, compliance, or achievement of agreed milestones, in accordance with the notice and reporting requirements of the grant agreement.

If a risk event necessitates a change to project activities, timing, or milestones, a variation request will be prepared and submitted in accordance with the grant agreement. The project recognises the Commonwealth’s rights to withhold payments, require remedial action, or step in to manage project delivery where serious risks to compliance or delivery arise. Risk monitoring and early mitigation are intended to prevent escalation to these remedies.

1.7. Continuous Improvement

This Risk Management Plan is a living document and will be updated throughout the project to reflect evolving risks and lessons learned. Residual risks are monitored to ensure they do not escalate to a level that could trigger suspension, reduction, or termination of the grant agreement.

2. Risk Register

The table below provides a risk register for the project. Likelihood and consequence are assessed on a qualitative basis (Low, Medium, High). The register will be reviewed and updated throughout the project lifecycle

REF	RISK CATEGORY	RISK DESCRIPTION	IMPACT	CONSEQUENCE	LIKELIHOOD	RATING	MITIGATION / CONTROLS	LIKELIHOOD	RATING	RISK OWNER
				INHERENT RISK				RESIDUAL RISK		
1	Scientific / Technical	Delay in synthesis and analysis of legacy datasets	Delayed Milestones, threat to delivery of outputs affecting stakeholder confidence, project credibility, and ongoing funding.	High	Medium	High	Early data audit, staged analysis plan, cross-institutional support	Low	Medium	Work Package Lead
2	Schedule	Delay in meeting publication and reporting milestones	Delayed Milestones, threat to delivery of outputs affecting stakeholder confidence, project credibility, and ongoing funding.	High	Medium	High	Clear milestone definition, progress monitoring	Low	Medium	Project Director
3	Financial	Expenditure misclassification or budget non-compliance	Funding recovery, audit non-compliance, adverse impacts on reputation and future funding.	High	Low	Medium	UTAS finance oversight, dedicated project officer, regular budget reviews, pre-approval of expenditure	Low	Low	UTAS Finance Manager
4	Data Governance	Failure to meet Antarctic Data Policy or FAIR requirements.	Data non-compliance, limited data discoverability and reuse, audit issues, project credibility, reputation, future funding eligibility.	High	Low	Medium	Dedicated data stewardship at IMAS/UTAS, experience of alignment with AADC standards, internal QA checks.	Low	Low	Data Lead
5	Consortium	Partner Underperformance	Delivery delays, reduced output quality, and increased burden on other consortium partners.	Medium	Low	Low	Existing ACEAS partnerships, defined deliverables, escalation pathways	Low	Low	Project Director

6	Personnel	Loss of key personnel affecting delivery	Loss of expertise, reduced project continuity, delays to deliverables, risk to outputs and milestone achievement.	Medium	Medium	Medium	Succession planning, role redundancy, cross-training	Medium	Low	Project Director
7	Personnel	Delay in recruitment	Gaps in resourcing, delays to activities, milestones, project delivery.	Medium	Medium	Medium	Few positions require open recruitment. Early commencement to recruitment	Low	Low	Project Director
8	Scientific / Technical	Insufficient High Performance Computing affecting delivery	Limit timely execution of computational workflows, impacting output quality, milestone achievement, project delivery.	High	Medium	High	National Computing Infrastructure (NCI) allocation through 2026. Early negotiation on NCI extension. Enter National Computational Merit Allocation Scheme competition. Use ANU partner allocation.	Medium	Medium	Project Director
9	Reputation	Negative public communications, media engagement, or misrepresentation of project findings or Commonwealth association	Reputational damage to the project, consortium, and associated Commonwealth entities, reduced stakeholder and public trust, increased scrutiny affecting project delivery and future funding.	High	Low	Medium	Clear communication protocols, dedicated and experienced Communication and Stakeholder Engagement Advisor, compliance with grant acknowledgement and approval requirements, internal review of public materials	Low	Low	Project Director
10	Personnel	Delay in contract execution	Loss of expertise, delays to activities, milestones, project delivery.	High	High	High	Provide bridge funding to consortium Partners to extend and maintain contracts.	Medium	Medium	Project Director
11	Safety and wellbeing	Impacts by public health risks to staff requiring change to ops environment managed within project (e.g., natural disaster, infectious disease)	In the event of a major public health event, some staff may become unavailable to deliver on the project.	High	Low	Medium	Avoid single point dependencies in project implementation plan and personnel.	Low	Medium	Project Director

12	Reputation	Limited stakeholder availability	Reduced ability to consult and disseminate findings	High	Low	Medium	Prioritise Tier 1 stakeholders and realistic engagement schedules	Low	Medium	Project Director
13	Reputation	Stakeholder engagement not aligned with project delivery	Delayed communications of key outcomes and deliverables	High	Low	Medium	Link engagement activities to milestones and outputs	Low	Medium	Project Director
14	Reputation	Fragmentation across consortium	Uncoordinated engagement and missed opportunities	High	Low	Medium	Clear governance, coordination and internal communication	Low	Medium	Project Director
15	Reputation	Over-commitment of beyond grant scope	Major project outcomes usurped in engagement and communication work	High	Low	Medium	Proportionate engagement aligned to funded activities	Low	Medium	Project Director
HIGHEST REMAINING RESIDUAL RISK								Medium		

Appendix I: Risk assessment tool rubric

			CONSEQUENCE (Project Impact)				
		Definition	The impact would pose some obstacles for the Project to achieve immediate objectives (within 3 months). **Impact managed as part of BAU.**	The impact would threaten the ability of the Project to meet its strategic objectives in the short term (within 6 months). **Impact managed by Executive Team.**	The impact would threaten the ability of the Project to meet its strategic objectives in the medium term (6-12 months). **Impact requiring Oversight Committee visibility and advice.**	An impact which significantly disrupts the Project from achieving its key strategic objectives, values, and ability to operate in the long term (1-2 years). **Impact requiring Oversight Committee visibility and advice.**	An impact which prevents the Project from continuing to operate.
LIKELIHOOD	**Frequency**	**Rating**	**Minor**	**Moderate**	**Major**	**Severe**	**Catastrophic**
	Likely to occur at least once a year (> 50% chance in any year)	**Likely**	**Mod**	**High**	**High**	**Ext**	**Ext**
	Likely to occur once in 2-5 years (25% - 50% chance in any year)	**Possible**	**Mod**	**Mod**	**High**	**Ext**	**Ext**
	Likely to occur once in 5-1 0 years (10% - 25% chance in any year)	**Unlikely**	**Mod**	**Mod**	**High**	**High**	**Ext**
	Likely to occur once in 10-50 years (2%-10% chance in any year)	**Rare**	**Low**	**Mod**	**Mod**	**High**	**Ext**
	Greater than 50-year event (< 2% chance in any year)	**Extremely Rare**	**Low**	**Low**	**Mod**	**High**	**Ext**

CONSEQUENCE		Consequence Rating (Project Impact)				
		Minor	**Moderate**	**Major**	**Severe**	**Catastrophic**
		The impact would pose some obstacles for the Project to achieve immediate objectives (within 3 months). **Impact managed as BAU.**	The impact would threaten the ability of the Project to meet its strategic objectives in the short term (4-6 months). **Impact managed by the Executive Team (ET).**	The impact would threaten the ability of the Project to meet its strategic objectives in the medium term (7-12 months). **Impact requiring Management Committee (MC) visibility and advice.**	An impact which significantly disrupts the Project from achieving its key strategic objectives, values, and ability to operate in the long term (13-24 months) **Impact requiring Management Committee (MC) visibility and advice.**	An impact which prevents the Project from continuing to operate.
CONSEQUENCE	Financial	<2% negative deviation from planned budget. Financial loss of up to $100K Impact requires minor change to the operational environment that can be managed as BAU.	2% - 5% negative deviation from planned budget. Financial loss of between $100K - $250K Impact requires moderate change to the operational environment that can be managed within budget by the ET.	5% - 8% negative deviation from planned budget. Financial loss of between $250K - $400K Project needs to activate part of the contingency funds to support deliverables	>8% negative deviation from planned budget. Financial loss of between $400K - $1M Impact requires significant changes and most of the contingency funds to be released to continue.	Whole of Project Income Statement impact exceeds available funding capacity of the Project.
	Reputational	Isolated incidents of dissatisfaction from end users, community members, Supporting or Delivery Partners or staff, Lead Agency, and funder.	Manageable impacts to the Project's local recognition/ reputation. Dissatisfaction from multiple Partners, Lead Agency, funder, or from multiple personnel cohorts. Heightened community concern with potential to escalate.	Manageable impacts to the Project's National recognition/ reputation. Permanent loss of minor Partner and/or significant reduction of personnel cohorts. Prolonged but manageable negative community sentiment or adverse local media coverage.	Prolonged but manageable impacts to the Project's international recognition/ reputation. Permanent loss of Key Partner and/or significant withdrawal of personnel cohorts. Prolonged significant negative community sentiment or adverse national media coverage.	Deterioration of the Project's reputation such that jurisdictions are unwilling to support continued collaboration, and the Project loses funder support.
	Safety and Wellbeing	**Work, Health, and Safety Risks**				
		The Project has no appetite for exposing personnel or community members to uncontrolled physical harm or failing to proactively address psychosocial hazards and risks.				
		Public Health Risks (Natural disaster, Climate related, infectious disease, epidemic, pandemic)				
		Short-term impacts to personnel that require minor operational changes managed as part of BAU.	Moderate impacts to personnel that require change to operational environment that can be managed within the ET.	Widespread impact to multiple personnel with an inability to deliver core services and operations across sites.	Widespread long-term impact to multiple personnel requiring significant change to Project operations.	Sudden or unexpected death of a high proportion of personnel.
	Environmental	Minor or short-term damage to a localised area or damage that ceases once the event is over.	Short-term impacts, where the ecosystem will recover quickly with or without intervention.	Relatively widespread medium-term impacts, requiring remediation, where ecosystem will recover once clean-up has been completed. Compromises project sustainability.	Medium to long-term and relatively widespread environmental effects.	Incident with permanent environmental damage.
	Privacy and Security	Unauthorised access to non-sensitive areas. Minor data breaches with no sensitive information. Minor physical damage. Temporary system downtime with no data loss.	Unauthorised access to restricted areas. Data breaches involving non-critical information. Moderate physical damage. System downtime causing minor operational delays.	Unauthorised access to highly restricted areas. Data breaches involving sensitive information Significant physical damage. System downtime causing significant operational delays.	Unauthorised access causing operational disruption. Data breaches involving highly sensitive information. Severe physical damage. Prolonged system downtime causing major operational disruption.	Unauthorised access causing complete operational halt. Data breaches involving critical and highly sensitive information. Catastrophic physical damage. Extended system downtime causing catastrophic operational failure.