Business Risk Maturity Tool

Introduction

Effective risk management is critical to sound governance[1], building a consistent appetite for and robust culture in risk, improving decision-making and maximising opportunity. When adopted and integrated by an organisation, risk information provides insights into and transparency over material operational, change/growth, disruptive and emerging upside and downside risks.

It is our vision that, at UNSW, understanding, evaluating and managing upside and downside risk will be central to decision making and will support efficient delivery of strategy and the pursuit of opportunity.

Realising the value of Risk Management

Effective risk management is based on strong foundations incorporating the following attributes. Adoption of these attributes or principles will assist the university to realise the related benefits.

Risk Management Attributes

1. Clear guidance on what is risk management, how it is to be applied and how tools are tailored to the needs of the area
2. Data is captured and analysed enabling insights and validation of risk information
3. The appropriate level of risk competency and capability exists across the University
4. Thought leadership promotes leading risk practices
5. Reporting stimulates foresight discussions
6. Executives and Governors are actively engaged in the management of risk
7. Risk is core to decision-making
8. Voicing uncertainty is part of our cultural norm

Figure 1: Risk Management Value Attributes

---

[1] ASX Corporate Governance Principles and Recommendations, ed 4, Feb 2019
Business Risk Maturity Tool V1 FINAL 2020.01.21

Risk Management Maturity Rating Table

The following table defines the maturity ratings used to rate each of the attributes/principles.

Table 1: Risk Management Maturity Rating Table

Maturity Rating	Description
Innovative	The organisation continually seeks new ideas and deploys creative thinking to further the effectiveness and integration of risk into the business. Risk is seen as an opportunity to innovate, which strengthens the focus on foresight risk.
Intelligent	The risk management framework, tools & templates are tailored to ensure integration with and alignment to the context, existing processes and maturity of the area, whilst maintaining the ISO 31000 principles. The Risk Appetite is integrated into decision-making. Risk discussions are mature and voicing uncertainty is a cultural norm.
Repeatable	The risk management framework, tools, templates & guidance are consistently applied. Risks are identified, assessed & monitored. Executives and Governors are engaged. Reporting is salient and draws on data and risk profiles.
Foundation	A risk management framework, risk process and tools are present. Adoption is dependent on Champions' engagement and not organisation-wide. The quality of output is variable.
Ad-hoc	Risk is considered when directed and tools are sought at this time. Guidance is provided on a case by case basis. Risk information is provided when requested and not integrated into reporting. A 'tick box' approach is prevalent.

The Risk Maturity Matrix (Table 2) is designed to enable each relevant area (i.e. Division, Faculty or Business Unit e.g. IT, EM, Finance) to self-assess their current risk management maturity. The results should be used to inform continual improvement as part of usual business planning, and related actions can be incorporated in the Risk Management Strategy for each area. It is noted that there are some units/activities where an imperative will be to reach a high level of maturity and others where this would not be required. Thus, multiple ratings for one unit can be seen given the nature of activities and tasks the Faculty, Division or Controlled Entity undertakes.

Instructions for Areas Conducting Risk Management Maturity Self-Assessments

1. Select appropriate area representatives and subject matter experts to jointly review the maturity rating table
2. Discuss the elements and related criteria. Then select the most appropriate description for your operation. (Note: where there is a range given multiple activities within your area, note these on the comments section of the form.)
3. Identify key areas of desired improvement and reflect this in your Risk Management Strategy (Appendix A)

Business Risk Maturity Matrix	Faculty / Division / Controlled Entity / Project Name:	School /Unit name:

Element: Leadership/ Culture

Rating: Sub-element	*Ad-hoc*	*Foundation*	*Repeatable*	*Intelligent*	*Innovative*
Governance	☐ Leaders inconsistently review their risk information ☐ Risk information is not formally used in decision-making forums ☐ Risk Committee interogates risk information in a cursory manner	☐ Leaders have oversight of risk information when it is part of management and project meeting papers ☐ Risk Committee reviews and seeks clarity over risk information to satisfy its Terms of Reference	☐ Leaders actively debate risk to ensure appropriate oversight and consideration of issues ☐ Decision-making is supported by an agreed risk appetite statement and risk profile information ☐ Council & sub-committees seek oversight of risk through reports and presentations by the appropriate personnel	☐ Leaders raise risk and opportunity considerations as part of BAU ☐ Council & sub-committees oversee risk through reports, sharing of information, deep dives and presentations on key topics	☐ Oversight of risk information is not reliant on standard reporting or scheduled presentations. Opportunities to engage in foresight discussions are pursued and shared across council and sub-committees to enhance the oversight of risk
Culture	☐ Adverse risk information is poorly received ☐ Risk information is considered only when it is requested by staff ☐ Relevant stakeholders & SMEs are inconsistently consulted about risk ☐ Risk information is poorly communicated beyond those who identify risks	☐ Leaders are willing to talk about risk but discussions are impacted by access to appropriate risk information ☐ Stakeholders & SMEs are engaged but their information is fragmented ☐ Limited dissemination of risk information to stakeholders	☐ Open discussions on risk and risk appetite are promoted by leaders ☐ Staff engage in risk management activities as part of BAU ☐ Risk discussions are inclusive (key internal and external stakeholders & SMEs are engaged) ☐ Risk discussions are not limited to the content of a risk profile document	☐ All layers of the organisation actively engage in risk management ☐ Voicing uncertainty is part of cultural norm and seen as a valuable part of discussions ☐ The Risk Appetite Statement is central to decision-making and reflect our values and visions ☐ Broad engagement and comprehensive sharing of risk information occurs	☐ Alignment of opportunities / activities to our Risk Appetite is part of BAU discussions ☐ Risk-reward discussions are part of the dialogue at UNSW ☐ Understanding opportunities, whilst comprehensively exploring and managing the unintended consequences and associated threats, is a key point of differentiation for UNSW
Continuous Improvement	☐ Risk & control improvement initatives are not well supported if not in budget	☐ Agreed risk & contol improvement initatives are supported when related to high risks	☐ Proactive identification of risk & control improvement initatives occurs as part of BAU	☐ Improvements to controls that enhance opportunities or limit risks are actively pursued	☐ Thought leadership promotes leading risk practices

Comments: *(Please clarify the reasoning for multiple ratings of a sub-element or issues that arise as part of assessing this element)*

Element: People/ capability					
Sub-element	**Ad-hoc**	**Foundation**	**Repeatable**	**Intelligent**	**Innovative**
Roles, responsibilities & accountabilities	☐ No formal risk champions exist for the area ☐ Risk management is seen as the responsibility of the risk function	☐ Risk champions are nominated or exist but have ad hoc engagement ☐ Risk management is seen as the responsibility of champions, those with high-risk roles or senior management	☐ Risk, Control & Action Owners are nominated and held to account ☐ Managers are clear about their roles & responsibilities in risk and are held to account	☐ All personnel are clear on their risk roles & responsibilities & are held to account for their performance & behaviour	☐ Individuals hold each other accountable for their risk performance
Capability	☐ Staff request risk guidance when directed ☐ Training is not considered	☐ Training is considered as participation in risk activities ☐ RM capability is dependent on the experience and background of personnel and the nature of the role	☐ RM capability development program is agreed annually for the area ☐ Specialist risk resources and SMEs from across the University are engaged	☐ Job descriptions contain risk capability requirements and personal KPIs include risk training goals ☐ Training is targeted, salient to different needs and accessible	☐ A training and capability model is established and implemented as part of BAU ☐ Cross-skilling of personnel within areas includes a capability for managing risk

Comments: *(Please clarify the reasoning for multiple ratings of a sub-element or issues that arise as part of assessing this element)*

Element: Process/ Tools					
Sub-element	**Ad-hoc**	**Foundation**	**Repeatable**	**Intelligent**	**Innovative**

Risk Assessment & Control	☐ Risk assessment (business, project and strategic) and control self-assessments are informal, ad hoc and seen as a 'tick box' activity
	
	☐ Potential impacts of disruptive/ extreme events are not formally assessed
		☐ Structured risk tools are adopted but the quality of content is variable. These include:
		  ☐ Operational risk assessment
		  ☐ Project Risk Assessment
		  ☐ Strategic Risk Assessment
		  ☐ Control self-assessments
		  ☐ Maturity self-assessment
		  ☐ Business Impact Aanalyses
		☐ Data (lag and lead indicators) is opportunistically used to inform/validate risk information
		☐ High-level, non BAU impact analyses (i.e. disruptive/ extreme events) and continuity plans are generated at the business level
		☐ Post Incident Reviews are completed but systematic learning is limited by a siloed approach or focused on compliance
			☐ Structured risk tools are adopted and provide a consistent level of content quality. These include:
			  ☐ Operational risk assessment
			  ☐ Project Risk Assessment
			  ☐ Strategic Risk Assessment
			  ☐ Control self-assessments
			  ☐ Maturity self-assessment
			  ☐ Business Impact Analyses
			☐ Data (lag and lead indicators) is formally captured to inform/validate risk information
			☐ The risk appetite is built into strategic decision making
			☐ Disruptive and extreme events are assessed using stress testing and scenario analysis
			☐ Post Incident Review learnings are identified but variably implemented or tracked
				☐ Risk tools are online, accessible and integrated across sub-specialist risk areas (i.e. compliance, safety, IT, Finance, operational)
				
				☐ Data (lag and lead indicators) is drawn upon to provide trending and benchmarking insights
				
				☐ Preventative, detective and continuity plans for disruptive and extreme events are current, comprehensive and tested as part of BAU
				
				☐ Post Incident Review learnings are identified and implemented, and improvments monitored
					☐ Online tools are integrated into core business processes/systems to ensure seemless management by stakeholders
					
					☐ A fully integrated program supporting organisational resilience is in place

Risk Monitoring & Reporting	☐ Risk reporting is completed under the requirement to contribute to the quarterly Risk Committee papers ☐ Risk is not a usual item in management meetings or papers	☐ Risk information is included in some templates (i.e. strategic initiatives, projects and Council / Sub-committee reporting) ☐ Agreed actions to mitigate risk are monitored by the area ☐ Leaders engage in the reporting of risk for their areas to support the consolidated Risk Committee paper	☐ Reporting of risk occurs across the Uni and Controlled Entities and includes Schools, Divisional Units, Major Projects, JVs and Alliances ☐ Leaders, HOS, Directors, CEOs of CEs include risk information in management reporting and to support decisions ☐ Leaders prepare and present at the Risk Committee and/or MB/SLT	☐ Risk reporting is partly automated and tailored to align to the needs (from a process level to Council/sub-committee level) ☐ Risk reporting includes comprehensive analysis of threats and opportunities	☐ Reporting is predominantly automated and linked to lead and lag data. It has a forward- looking view to stimulate foresight discussion
Score	. . /16	/22	/17	/16	/11

Comments: *(Please clarify the reasoning for multiple ratings of a sub-element or issues that arise as part of assessing this element)*

Appendix A:

Risk Management Strategy for *(enter in Faculty/ Division, School/Business Unit, JV and Controlled Entity name)*

Date:

Introduction

Drawing on the outcomes of the risk maturity self-assessment, an agreed set of actions to mature the risk capability and performance will be captured in this document and signed off by each Faculty, Division, School/Business Unit, Joint Venture and Controlled Entity.

To ensure that the strategy can be achieved, consideration of budgets, engagement requirements of personnel and the need to enhance risk management performance will be necessary. These considerations will also be important in determining the number of activities that will be pursued in the year.

Objective	Actions	Owner	Timeframe	Monitoring Forum and frequency	Status *(On schedule; delayed; Not started; retired)*
Build capability in risk management for all project owners	Secure training and tools for project owners	FED / UPO	Q1 2020	Mthly at Faculty Leadership Team	Not Started

Approval

	Name & Signature	Date
Author		
Owner		
Approved by		
Endorsed by		