



The Deakin University Risk Management approach

moving toward enterprise risk management



Outcomes

1. Outline the Risk Management Program
2. What is Risk Management?
3. Deakin University Risk Assessment methodology
 - Terminology
 - Working example
 - Risk Register
4. Avoiding Common pitfalls

Risk Management Program

Risk Management Framework

- > Policies and procedure
- > Risk criteria
- > Optional proformas

Risk Registers

- > RiskManager

Risk and Compliance Management Subcommittee

- > Annual review of all risk registers

www.deakin.edu.au

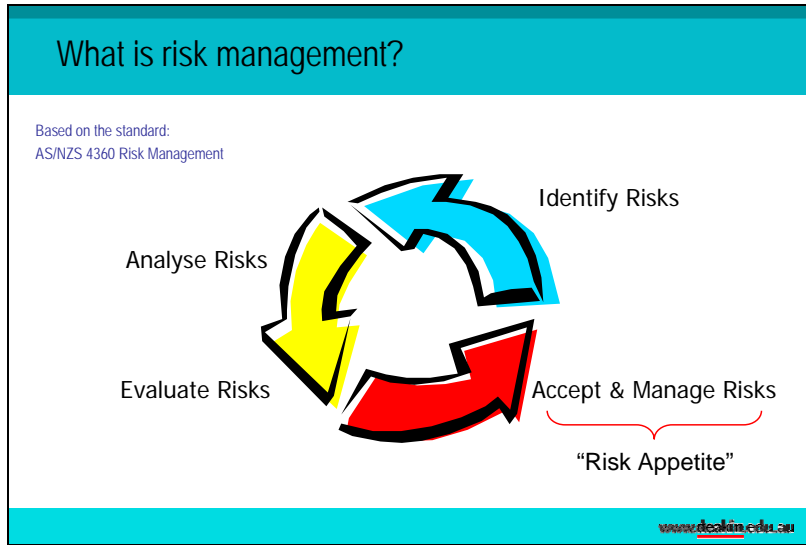
The **Risk Management Framework** can be found on [The Guide](#). You may wish to make yourself familiar with these documents:

- Risk Management Enabling Policy
- Risk Management Operational Policy
- Risk Management Procedure
- Risk Management VET Operational Policy
- Risk Management VET Procedure

You will need to obtain a copy of the **Deakin University Risk Criteria** – also available on the [Finance and Business Services Division website](#).

[Risk Registers](#) are the method by which Deakin University captures identified risks, more information can be found on page 9.

The [Risk and Compliance Management Subcommittee \(RCMSc\)](#) amongst other items, reviews the effectiveness of the Risk Management Program. The RCMSc also conduct formal reviews of all organisational area risk registers guided by completed copies of the Risk Register Review Tool.



Risk Management is about the **logical and systematic method** of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risks associated with the activities, functions and processes of Deakin University to minimise loss and maximise opportunity.

The **Risk Management approach** is applicable to all of the University's activities and functions, and is in some instances prescribed by legislation. The approach facilitates:

- Improved decision making and planning;
- Enhanced identification of opportunities and threats;
- Pro-active rather than re-active risk management;
- Improved allocation and use of resources;
- Compliance program; and
- Corporate governance

The Risk Management program and Risk Registers cover events which relate to the University's strategic objectives and organisational processes, including:

- Teaching and learning;
- Research and research training;
- Internationalisation;

- Recruiting and retaining staff;
- Community responsibilities
- Communication and marketing;
- Resources, infrastructure and services;
- Information Technology;
- Occupational Health and Safety;
- Environmental issues;
- Emergency management,
- Public risk and liability;
- Ethics, fraud, security and probity issues;
- Purchasing and contract management;
- Operations and maintenance systems;
- Project management

Risk Appetite is all about determining whether Deakin University believes a risk to be tolerable or not. A number of factors impact on this, notably the residual risk rating (for more on this, see page 5 and 8), but it also depends on the potential benefits the University can gain by accepting the risk as it is.

Methodology - Terminology

Risk Category

- **Select** the 'best' description of exposure

Corporate Objective

- **Select** the relevant Strategic Objective

Risk Title

- **Describe** the 'essence' of the risk

Contributing Factor

- **Describe** the influencers

www.deakin.edu.au

In order to adequately describe risks a number of criteria should be used. At Deakin University we describe risks through a category framework making reference to the relevant strategic objective. You also need to take care to ensure that the title you select adequately describes the event so that the risks can be understood in broad terms. To help you do this, consider asking questions such as a risk 'to what', 'of what' and 'from what'.

The **Risk Category** is selected from:

- Financial Management Risk
- Assets Management Risk
- People Management Risk
- Academic Process Risk
- Information and Management Systems Risk
- Compliance with External Regulation and Legislation Risk
- Compliance with Internal Policies Risk

The **Corporate Objective** captured reflects one of the University's Strategic Objectives:

- Teaching and learning
- Research and research training
- Internationalisation
- Recruiting and retaining staff
- Community responsibilities – rural and regional engagement;
- Communication, marketing and positioning
- Resources, infrastructure and services

Risk impact refers to the outcome of an event or situation expressed in terms of loss, injury or disadvantage before any control measures are introduced.

Likelihood refers to the probability and frequency of the event occurring before any control measures are introduced.

Methodology - Terminology

Impact

- Select the result or effect of the event/opportunity

Likelihood

- Describes the probability of the event/opportunity

Inherent Risk

- Combination of impact & likelihood

Controls

- Implemented item to control either consequence or likelihood

Residual Risk

- Combination of impact, likelihood & controls

Actions

- Item to be implemented to control either impact or likelihood

}

From Risk Criteria

www.deakin.edu.au

The **inherent risk rating** describes the combination of the impact and likelihood. The inherent risk rating recorded is based on the Risk Criteria computation and RiskManager will automatically calculate it for you.

Control(s) refers to the mechanisms currently in place to minimise either the impact of the event or the likelihood of the event occurring. See the next page for more details on the concept of control and actions.

The **residual risk rating** describes the combination of the consequence rating, the likelihood rating and the control rating. The residual risk rating recorded is based on the Risk Criteria computation and RiskManager will automatically calculate it for you. The residual risk rating guides the requirement for the implementation of actions.

1. A **very high** residual risk requires attention. Consideration by PRC is required, generally unacceptable - save in extraordinary circumstances, detailed research and planning into appropriate actions is required to mitigate the risk.
2. A **high** residual risk requires attention of the organisational head. Appropriate actions are nearly always required to mitigate the risk. Management need to ensure that necessary mitigation actions are carried out and the risk does not

increase by actively monitoring any changes to the control environment, consequence and likelihood.

3. A **medium** residual risk is tolerable, management to ensure that the control environment, consequence and likelihood do not substantially change. Consider the implementation of any practicable actions.
4. A **low** residual risk is acceptable. You should only implement actions if there is a clearly quantifiable cost benefit.
5. A **very low** residual risk is acceptable; actions are not required as resources are likely to be grossly disproportionate to reduction achieved.

Actions are the mechanisms to be implemented to minimise either the consequence of the event or the likelihood of the event occurring. Each item/action must be described including responsibility, timeframes and status.

In order to evaluate risks and ensure a consistent approach across the University, we have developed the Deakin University Risk Criteria—impact, likelihood and controls must be ‘rated’ using this tool. We’ll cover this in more detail later.

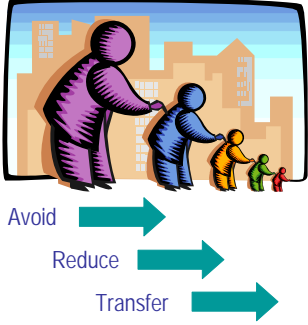
Methodology - Control concepts

Reduce Risk through Hierarchy of Control

Controls are classified as

- Detective
- Interdependent
- Preventative
- Reactive

An action migrates to a control once it is established



www.deakin.edu.au

The whole concept of control is to avoid the risk if possible, if you can't reduce the risk and finally if nothing else can be done, transfer the risk. Some risks Deakin wants to take and some it doesn't, in other words, this is our 'Risk Appetite'.

Controls are classified under one of 4 groups. It's prudent to have controls under each of the groupings.

1. **Detective** controls relate to investigations, they are established to spot error or omissions after the event, eg checks; financial reconciliations; audits; monitoring; fire alarms.
2. **Interdependent** controls are those relying on involvement of other divisions/faculties to control. You must talk to the responsible areas before assuming they can implement such a control.
3. **Preventative** controls are established prior to an event occurring, eg qualified staff; position descriptions; training; performance measures; strategic and operational plans; policies and procedures; codes of conduct; security.
4. **Reactive** are controls where there are no tangible actions to address the event and/or transference of liability, eg contingency plans; backups; recovery plans; insurance

When considering actions, make reference to the concept of 'reasonably practicable' taking into account:

- The likelihood of the risk identified eventuating;
- The consequence of the risk identified eventuating;
- What the assessor(s) know, or ought to reasonably know, about the risk and any ways of eliminating or reducing the risk;
- The availability and suitability of ways to eliminate or reduce the risk; and
- The cost of eliminating or reducing the risk

The priority for determining the most effective action is as follows in the descending order:

- Elimination
- Substitution
- Engineering
- Administrative
- Personal Protective Equipment
- Transfer

Again it's prudent to select a combination of actions to eliminate or reduce the residual risk. Preference should be given to the higher order risk control measures.


Once implemented and functioning, actions should be reclassified as a control and the control rating reassessed.

Risk Criteria, Risk Register & Risk Assessment

Establish the risk category, corporate objective, title and contributing factors

Then

- 1 Determine Impact Rating
- 2 Determine Likelihood Rating
- 3 Inherent Risk Rating
- 4 Current Controls



www.deakin.edu.au

Need a reminder on **risk categories**, **corporate objectives**, **the risk title** or **contributing factors**? Go back to page 4.

Impact rating - is the result or effect of an event against five impact ratings. Each category of outcome (OHS, Financial, Environmental, Reputation, Outrage & Media and University Performance) must be considered. There are 5 ratings – catastrophic, major, severe, modest or minor. The impact rating recorded is the highest rating consequence from the five categories.

Risk Criteria - Impact

		Measuring Risk - IMPACT				
		UHS	Financial	Environmental	Reputation, Outrage & Media	University Performance
Catastrophic	Catastrophic	Catastrophic	Catastrophic	Catastrophic	Catastrophic	Catastrophic
Major	Major	Major	Major	Major	Major	Major
Severe	Severe	Severe	Severe	Severe	Severe	Severe
Modest	Modest	Modest	Modest	Modest	Modest	Modest
Minor	Minor	Minor	Minor	Minor	Minor	Minor

Impact = MAJOR

www.deakin.edu.au

Likelihood refers to the probability and frequency of the event occurring before any control measures are introduced. There are 5 ratings – almost certain, likely, possible, rare or almost impossible. The likelihood rating recorded is based on the overriding definition.

Risk Criteria - Likelihood

		Measuring Risk - LIKELIHOOD				
		UHS	Financial	Environmental	Reputation, Outrage & Media	University Performance
Almost certain	Almost certain	Almost certain	Almost certain	Almost certain	Almost certain	Almost certain
Likely	Likely	Likely	Likely	Likely	Likely	Likely
Possible	Possible	Possible	Possible	Possible	Possible	Possible
Rare	Rare	Rare	Rare	Rare	Rare	Rare
Almost impossible	Almost impossible	Almost impossible	Almost impossible	Almost impossible	Almost impossible	Almost impossible

Likelihood = POSSIBLE

www.deakin.edu.au

The **inherent risk rating** describes the combination of the impact and likelihood as one of 5 Inherent Risk ratings – Very High, High, Medium, Low or Very Low. The inherent risk rating recorded is based on the matrix computation and RiskManager will automatically calculate it for you.

Risk Criteria – Inherent Risk

Inherent Risk = HIGH

www.deakin.edu.au

Control(s) refers to the mechanisms currently in place to minimise either the impact of the event or the likelihood of the event occurring. They need to be described accurately and are Excellent; Very Good; Good; Medium; Poor; or Out of control. See the previous page for more details on the concept of control. Controls can be ongoing items.

Risk Criteria – Control Rating

Inherent Risk = HIGH

Control = GOOD

www.deakin.edu.au

Risk Criteria, Risk Register & Risk Assessment

- 5 Residual Risk Rating
- 6 Actions
 - Guided by "Risk Appetite"

Then
Sign Off
Entry into Risk Register or Compliance Register*

**Legislative Risk Assessments only*

www.deakin.edu.au

Residual Risk Rating - Describes the aggregate of the impact, likelihood & control ratings as one of 5 Residual Risk Categories – Very High, High, Medium, Low or Very Low.

The residual risk guides the review cycle of each and every risk within the Risk Registers and links to our Risk Appetite:

- **Very High Residual Risk**– PRC have endorsed and monitored at each RCMS meeting (i.e. 1/4ly)
- **High Residual Risk** – Organisational head has endorsed, monitored at every 2nd RCMS meeting and advised to PRC annually
- **Medium Residual Risk** – ongoing management monitoring, monitored in RCMS risk register review groups
- **Low & Very Low Residual Risk** – ongoing monitoring by responsible person, monitored in RCMS risk register review groups

Risk Criteria – Residual Risk

RESIDUAL RISK CATEGORY	CONTROL STATUS	ACTION REQUIREMENTS
Very High	Out of control	Immediate action required to reduce the risk to a level that is acceptable to the University. The risk register owner must report the risk to the PRC at the next meeting.
High	Out of control	Immediate action required to reduce the risk to a level that is acceptable to the University. The risk register owner must report the risk to the PRC at the next meeting.
Medium	Out of control	Immediate action required to reduce the risk to a level that is acceptable to the University. The risk register owner must report the risk to the PRC at the next meeting.
Low	Out of control	Immediate action required to reduce the risk to a level that is acceptable to the University. The risk register owner must report the risk to the PRC at the next meeting.
Very Low	Out of control	Immediate action required to reduce the risk to a level that is acceptable to the University. The risk register owner must report the risk to the PRC at the next meeting.

Residual Risk = MEDIUM

www.deakin.edu.au

Actions describe the mechanisms to be implemented to minimise the either the consequence of an event or the likelihood. Each item/action must be described including responsibility, timeframes and status. If you nominate another division / faculty / institute as responsible for an action, you must discuss it with them and gain some kind of agreement in relation to implementation, prior to including it on your Risk Register.

Don't forget, once you've implemented an action effectively it becomes a control.

Once the assessment has been completed it needs to be **"signed off"** by the assessors' supervisor/risk register owner and also the person responsible for the risk (if not one and the same).

One last item to note, if you've just completed a risk assessment required by legislation, it should be recorded as a reference in your compliance register, **not** your risk register.

Risk Register

Deakin University's Risk Register framework:

- > University
- > Organisational
- > Area (optional)

All identified risks captured in your Risk Register*

Annual Risk Register Review

- > Risk & Compliance Management Subcommittee; or
- > Risk & Insurance Manager

*excluding Legislative Risk Assessments

www.deakin.edu.au


The Deakin University Risk Register framework comprises three levels:

- **University Risk Register** - captures risks related to the University as an entity; or risks very broad in nature; or risks with multiple responsible members of the Senior Executive. This register is developed by PRC with input from the Manager, Strategy and Risk and the Audit and Risk Committee.
- **Organisational Risk Registers** – capture risks related to a specific division / faculty / institute. These registers are developed by each organisational area and regularly reviewed by the RCMS. Advice in relation to content and rating is available from the Risk and Insurance Department.
- **Area Risk Registers** - optional register, which captures risks specific to a team or functional area within a division / faculty / institute. Advice in relation to content and rating is available from the Risk and Insurance Department.

You should use your risk register to capture all the identified risks within your area of responsibility.

Each year, you will be asked to participate in a **review of your Risk Register** by the RCMSc. These reviews are conducted by one of the one of the three Risk Register Review (RRR) groups. The RRR groups have a standard checklist, which will be provided to you or you can access it here [Risk Register Review Tool](#). Of course, the Risk and Insurance Department are also available to assist you to conduct an informal review of your Risk Register.

Risk Register



Deakin University's Risk Register is [RiskManager](#)

RiskManager

- > Contains all Risk Registers
- > Web based database
- > Administered by Risk and Insurance Department
- > Individual training available

www.deakin.edu.au


RiskManager is the electronic web-based database administered by the Risk and Insurance Department which captures all Risk Registers and Compliance Register.

You'll need to be set up to use RiskManager, just contact the Risk and Insurance Department

on ext 68112. A basic training package may be found on the [website](#) and individual training is available...just ask.

Working example...

Identify <ul style="list-style-type: none">> group brainstorm – is it a risk?	1. Group hazard identification brainstorm
Analyse <ul style="list-style-type: none">> quantitative – risk criteria	2. Small group risk assessment
Evaluate <ul style="list-style-type: none">> actions?	3. Common pitfalls
Accept, manage <ul style="list-style-type: none">> risk appetite> ongoing monitoring?	



www.deakin.edu.au

It is far easier to identify risks with a group of knowledgeable staff from your division/faculty, not just members of the management team.

Hazards may be identified through audits, reviews, inspections, observations, incident reports, incident investigation, contract reviews,

legislation, complaints, new work practices, new equipment, facilities or buildings and organisational analysis.

You may wish to utilise formal techniques to help your team identify hazards. Tools including brainstorming, flowcharting, system

Deakin University Risk Management Guidelines

design review, operational modelling or hazard and operability studies (HAZOP) are worth considering.

You could also try asking the following questions:

- Who are our major stakeholders or customers?
- What services do we provide?
- How do we know that goals are being achieved?
- What are our major strengths, weaknesses, threats and opportunities?
- What are the significant internal and external environmental factors impacting on our team?
- What issues have been reported?
- What key issues have emerged from previous inspections, audits or reviews?

If your identified hazard has the potential to place the University at risk of a legal, financial, moral or statutory penalty, you need to include it on your Risk Register – unless of course it's a hazard identified in legislation which requires a risk assessment – then it goes on your compliance register.

If after further analysis there is a negligible level of risk to the University, then this “hazard” becomes an issue that can be addressed at a divisional/faculty level.

Should a hazard contain multiple facets, it may be necessary to present each hazard as a separate risk assessment or item on the risk register.

Including your hazards on your **Risk Register** or completing a **Risk Assessment** is simple, just work through the process of:

1. Determining and recording your **impact rating** (from the Risk Criteria)
2. Determining and recording your **likelihood rating** (from the Risk Criteria)
3. Using the Deakin University Risk Criteria to ‘calculate’ the **inherent risk rating**

4. Describe and record the controls you already have in place to mitigate the risk, then determine and record your **control rating** (from the Risk Criteria)
5. Using the Deakin University Risk Criteria to ‘calculate’ the **residual risk rating**
6. Identify any **actions** that can be taken to further mitigate the risk and record them – you need to assign timeframes and responsibilities.

There are a number of **common pitfalls** with Risk Assessments and Risk Register. You should try to avoid the following:

- Carrying out a risk assessment to attempt to justify a decision that has already been made
- Using a generic assessment when a site specific assessment is needed
- Carrying out a detailed quantified risk assessment without first considering whether any relevant good practice was applicable, or when relevant good practice exists
- Carrying out a risk assessment using inappropriate good practice
- Making decisions on the basis of individual risk estimates when societal risk is the appropriate measure
- Only considering the risk from one activity
- Not using a team or the people with practical knowledge on the ‘risk’
- Failure to consider all possible outcomes
- Inappropriate use of data
- Inappropriate definition of a representative sample of events
- Inappropriate use of risk criteria
- Not doing anything with the results of the assessment
- Not linking hazards with risk controls
- Not monitoring that controls identified are or remain effective
- Not following up on the implementation of actions

Where to from here...

What do I do with my Risk Register?
Get ready to participate in Risk Register Review
Refer to Deakin Risk Management Program documentation
Contact Risk & Insurance Department
> 68112
> insure@deakin.edu.au



www.deakin.edu.au

Once you've completed your Risk Register, you should be using it as a **Risk Management tool** within your area. So what does that mean?

- Align the content of your Risk Register with your strategy and operational plans to maximise your effectiveness
- Use your Risk Register as a decision making tool – is the proposed action a 'good idea'?
- Think about the links across your Risk Register items – which are critical for your success? Focus on managing those items.
- Apply the concepts of risk optimisation – implement and track your actions, re-rate your risks

- Monitor the effectiveness of your existing controls – are they all still relevant? Are they all still functioning? Are they all still contributing to the control of the risk?
- Using your risk register as a tool to support your budget bids.

The Risk Management Program documentation contained on [The Guide](#), just search for 'risk management' and the [intranet site](#) can provide you further information.