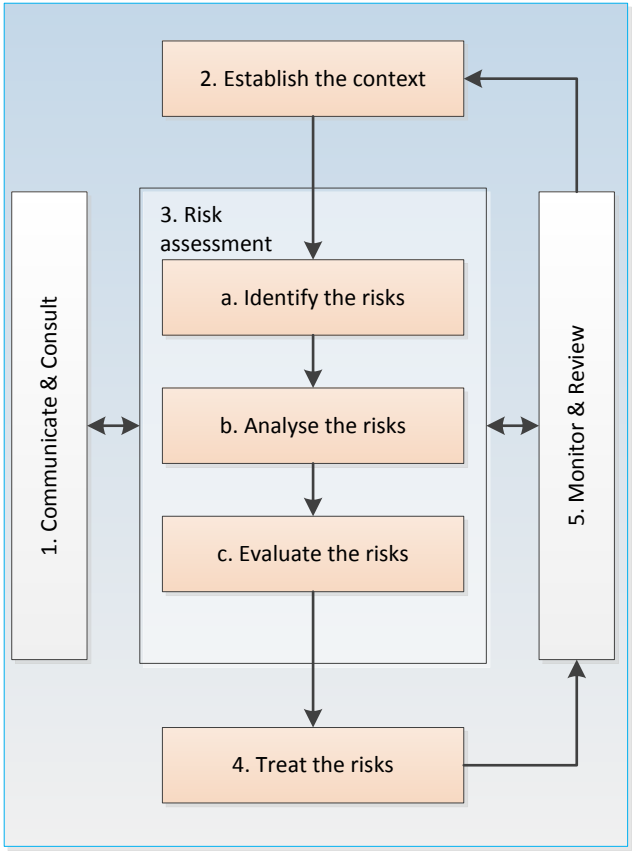
How to conduct a risk assessment

Process
for managing risk



How to conduct a risk assessment

1. COMMUNICATE AND CONSULT

It is important to consider the knowledge, experience and role of others when determining what risks are relevant to the activity. Conducting a workshop with internal and external stakeholders will provide the best collaborative assessment. Consider consulting with, but not limited to, the following at any stage of the risk management process:

subject matter experts	operational staff	end-users
people who do the job	event coordinator	project manager
project sponsor	decision makers (executive and managers)	

2. ESTABLISH THE CONTEXT

The risks being identified should relate to the activity being undertaken e.g. business operations, a project, a procurement or an event. Developing a 'Risk Context Statement' will assist in defining the activity and understanding the risk. Consider:

- scope, goals and objectives
- decision making processes
- systems and dependencies
- resource availability
- environmental factors.

What information is available?

Gather any relevant documents that may assist in identifying risks relevant to the activity you are assessing, these may include:

- strategic or operational plans
- policies and procedures
- project plans
- audit reports and recommendations.

3. IDENTIFYING THE RISKS

The process of finding, recognising and describing risks:

i. A **description** of the risk is the event

- what can happen? Consider appropriate language e.g.

Failure to…	Breach of…
Damage to…	Loss of…
Inadequate…	Insufficient…
Inability to…	Lack of…
Exceeding (authority, delegations, contract price etc.)…	

ii. The **source/cause**

- is the source, driver and contributors
- what causes the risk - how can it happen?

e.g. the source of the risk ***Damage to a building*** could be:

Natural disasters	Flood
Fire	Earthquake

e.g. the source of the risk ***Breach of legislation*** could be:

Lack of training and understanding by staff.
Time and resourcing constraints.
Poor control environment.
Deficient policies and procedures to support legislation.
Lack of monitoring and reporting.

iii. The **impact/outcome**

- is the consequence of the event/activity
- if what can happen does happen?

The inclusion of the consequence summary in the risk description supports the consequence rating chosen when analysing the risk. It also allows a view to be formed as to what is being managed.

The consequence should be described in its most *usual form* and not the *extreme form*.

e.g. the consequence of ***A paper cut*** is:

- *usual form*: cut not requiring first aid treatment
- *extreme form*: cut resulting in an infection, blood poisoning and death.

Note: if the risk described has ***no consequence*** or it ***can't ever happen*** then what you have described is not a risk.

iv. Assign a **Risk Owner** as it is important to assign accountability to ensure ongoing management of the risk.

e.g. Project Manager, Vice-President Governance & Development or Dean, Faculty of Business, Government and Law.

4. ANALYSING THE RISKS

i. **Risk controls currently in place -** the first step in analysing or rating risks is to consider what we are currently doing to manage the risk (i.e. our current risk controls), for example:

- policies and procedures
- delegate approval, monitoring and review
- regular training and development.

ii. The **Inherent risk rating** assesses the risk at how it is now, taking into account our current controls.

Using the UC Risk Matrix, determine the following:

- Step 1 **- Consequence** – what is the consequence level of the risk occurring in its most *usual* form?
  Consider the consequence in terms of the categories on the Risk Matrix (i.e. reputation, financial, teaching and learning, legal and compliance etc.)

  e.g. where a risk may result in a breach of legislation and damage to the University's reputation at a national level the consequence rating would be '*4 – Major'.*

- Step 2 - **Likelihood** – determined by the likelihood of the consequence of the risk occurring.

  e.g. where the risk may occur every 1- 5 years it would be '3 – Possible'.

- Step 3 – rate the risk using the UC Risk Matrix

Consequence x Likelihood = Risk Rating
4-Major x 3-Possible = High

5. EVALUATING THE RISKS

This is determining whether the current risk is acceptable or whether we need to take further action to manage the risk.

Using the **Control Effectiveness Rating (CER)** consider whether what we are currently doing to manage the risk is sufficient or should we be doing more? These can be evaluated as (refer to Risk Matrix for definitions):

- Inadequate
- Room for Improvement
- Adequate.

6. TREATING THE RISKS

If the CER is rated as 'Inadequate' or 'Room for Improvement' we need to determine what else we could be doing to manage the risk.

i. **Actions to be taken,** or additional controls, can be implemented to:

- **avoid** the risk by ceasing the operation (often not a viable option)
- **reduce** the risk e.g. through:
  - implementing policies, procedures, segregation of duties
  - implementing plans or planning processes (e.g. communication plans, business continuity plans)
  - conducting formal reviews or audits
  - inspection and monitoring of processes, activities and events
- **share** the risk e.g. through:
  - taking out insurance policies
  - contracting/outsourcing arrangements.

ii. Assign a **Risk Treatment Owner** who will be responsible for implementing any additional actions to be taken.

iii. The **Residual risk rating** is then determined. This is what the risk level will be after additional treatment actions have been implemented. The Residual risk rating can be assessed using the UC Risk Matrix and the same calculation process as the Inherent risk rating:

Consequence x Likelihood = Risk Rating
3-Moderate x 3-Possible = Medium

iv. Using the **Control Effectiveness Rating (CER)** consider whether what we intend to do to manage the risk will be sufficient or is there more we could be doing?

*** Risk Treatment Action Plans** – must be developed for all risks inherently rated as Extreme or High. The action plan includes:

- tasks to be undertaken to manage risk
- due dates or milestones for when actions should be completed
- the Treatment Owner who is responsible for implementing the treatment action.

7. MONITOR AND REVIEW

Risk registers should be **reviewed every six months**, at key project/event milestones or more frequently when there is a major environmental change *e.g. implementation of a new policy.*