RISK GUIDE NUMBER 3

A GUIDE TO PUTTING TOGETHER A RISK REGISTER

Assurance and Compliance Section

October 2016

INTRODUCTION

One thing in risk management that often causes concern is how to put together and use a risk register. People worry about producing long lists of things that don't really add anything to managing anything. Risk registers often don't get updated properly, so the effort in compiling them then becomes time wasted. Needless to say, these types of results are ones we all want to avoid.

This guide provides details on producing a risk register to avoid these problems. It focuses on having a register that adds something to the management of your operations.

We've also tried to make this guide jargon-free. Risk management has a lot of buzzwords! We've tried to exclude these as far as we can. We hope this will make this guide a lot easier for you to use. However, we know some people just find this kind of thing a little abstract or daunting. So, we're always ready to help you. We'll post things on the intranet, but will always try to meet you whenever possible. If you're really busy, drop us an email at ac@usp.ac.fj. We'll get back to you as soon as we can.

Director of Assurance and Compliance

October 2016

WHAT DO IN NEED TO DO BEFORE I SET UP A RISK REGISTER?

You need to have done the following things:

- Thought about the process for doing a risk assessment (see Risk Guide 1).
- Undertaken a process of risk identification (see Risk Guide 2).

WHEN IS IT A GOOD IDEA TO HAVE A RISK REGISTER?

Here are two broad categories that can determine if it's a good idea to have a risk register:

- **A big and/or important project:** These usually involve a lot of different processes. They also often have internal and external resources being involved in the delivery. A risk register is good at tracking these resources.
- **When you manage a budget or area of activity:** This can range from where you have a budget, to being in charge of an activity. A risk register can help in monitoring how resources are used to manage risks to your objectives.

WHAT CAN A RISK REGISTER DO AND NOT DO FOR ME?

The following table gives a general list of what a risk register can do and what it can't do. It is not a complete list. However, it gives some pointers.

What my risk register can do	What my risk register cannot do
It can be a clear summary of my key risks, which I can periodically update	It cannot be a full risk analysis. It's a high level summary. The full analysis backs the register up.
It's a great tool for reporting the current status of individual risks, facilitating discussion about them and causing action to be taken.	It cannot be a substitute for actively managing the risk itself. It is a summary record of that management.
It can be used to discuss the assessed risk level for my activities with my line managers. We can then agree actions to mitigate risks.	It cannot be a static record of how risk is managed. It needs to be kept up to date. Then, you and your managers can rely on it.
It can record my controls to manage a specific risk.	It cannot be the control over managing the risk itself.
It can record my planned actions to improve my controls.	It cannot be the control over managing the risk itself. It is a summary record of your controls.
It can record any assurances I have that the controls are working.	It cannot be the primary source of assurance about a specific risk on the register. It is part of the risk management framework.
It can be a summary record of assurance that I'm controlling the risk in the way I want. It can also show my controls cause the risk to be mitigated.	It cannot be the assurance itself. That is independently assessed and recorded on the register in a summary form.
It can list future actions and the people responsible for causing the risk to be mitigated.	It is not the future action itself. A good discussion of the register can help in deciding a course of action.

WHAT SHOULD I PUT ON MY RISK REGISTER?

The following table gives you an idea about what you should and should not put on your risk register:

Put this on your risk register	Don't put this on your risk register
Important risks to your objectives, whether from current operations or new opportunities.	Minor day to day issues that are managed by day-to-day supervision.

The important principle here is not to clutter your register with lots of relatively unimportant issues you manage day to day. Keep your register for really important risks to objectives. This will keep it smaller and easier to update. It will also mean your assessment of risk for the bigger risk items is more regular and detailed. That's appropriate, as these are the 'show stoppers' to you meeting objectives and targets.

IS THERE A TEMPLATE THAT I CAN USE?

Refer to Appendix A. The rest of the guide will explain the various key columns.

- Remember: As noted in Guide 1, the first step is to 'Understand the risk context'. This is important to ensure you are considering the right risks.

RISK# and RISK DESCRIPTION:

The risk# is a unique identifier. Normally starting at 1 and continue as 1 up number.
The risk description must clearly describe the "Risk". This is to ensure the risk is captured correctly providing a good understanding of the risk for future decisions.
The risk description should not be a problem, cause of the risk or effect/consequence of the risk.

- Problem/issue: Has already occurred and must be dealt with. No longer a risk.
- Cause, Risk, Effect: Refer to Guide 2. This document provides tips identifying these.
    - Note: The cause can be used to determine the best option(s) to treat your risks. If more than one option is available, review each and select the most appropriate (and effective) considering risk rating, budget, time, resources etc.

RATINGS:

Risks will be rated using the residual risk / current risk: This is the risk after controls have been taken into account or also known as risk remaining after treatment.

HOW CAN I GET CLEAR IN MY MIND WHAT'S REALLY IMPORTANT?

Refer to the Risk Criteria we are using across the university community to rate **risk** at an organisation level. The Risk Matrix is relationship between the likelihood and consequences**.**

- Required action taken is noted for each level of risk (extreme, high, medium and low)
- Example: Anything red is what gets reported to the Senior Management team, Council and Council Committees via the university's key risk register.
- This is only a guide as the nature of the risk and effectiveness of controls plays a role determining the appropriate action.

WHEN I RATE 'LIKELIHOOD' AND 'CONSEQUENCE', WHAT AM I RATING?

- What we're initially looking at in our risk register is how risky you think the activity is, given controls in place at the moment. In risk management jargon, that's called the 'residual risk'. So the 'current risk' columns are based on your view of 'residual risk'.

  You make your evaluation in the same way, but now you're looking longer term.

WHAT GOES IN THE 'EFFECTIVNESS CONTROLS' COLUMN?

This often causes a little confusion. Here's a basic description to help you.

- A control is, basically, something that directs something a particular way or stops something from happening. For example, getting something countersigned ensures compliance with procedure and stops one person from doing something without any checks. There are always really important controls that ensure the objectives of an activity are met and procedures followed. These are the 'key controls'.
    - In your Risk action plan: The existing key controls should be listed.

ARE THE CONTROLS EFFECTIVE?

- When you assess an activity, you may find there is an area of the process that doesn't really have any direction or where a bad thing could happen. These bad things could affect achieving an objective For example; imagine an unlocked tin with lots of cash in it. This would be a gap in control considered weak controls. The bad thing is it could be stolen. This would be against an objective of securing all cash. Where there are things like this, you need to record them.

- You might think you've got good controls. However, what evidence do you really have that they work? You might feel that, in some areas, the level of assurance is not really enough. These are gaps in assurance and should be listed. A good way of

thinking about this is that a key control should be matched to an assurance. It's a good way of initially identifying where you need further assurance.

- All managers want to know their controls are working properly. There are all sorts of ways of doing this. A couple of examples are independent audits and management reports. These let managers know if the controls enable any identified risk to be managed effectively. These types of things are known as 'assurances'.

WHAT ARE RISK ACTION PLANS?

Action plans should match the gaps in control and assurance you've identified. They enable you to state how gaps can be closed. That provides assurance to your line manager that identified gaps are being addressed.

A standard template has been provided to ensure reporting is in a standard format:

- Detail risk description: This must clearly explain the risk ensuring everyone reading the Risk action plan understands the risk. This is critical to avoid misunderstandings and confusion. Also incorrect controls are identified.
- Risk Drivers: What will cause the risk to materialise. This information is important to assist identify controls to manage the risk.
- What controls are in place: What are you currently doing to manage this risks (Example controls: policies, procedures, task lists, specific forms
- What is the effectiveness' of the controls: How are the controls working considering effectiveness and efficiency? (i.e. strong, moderate, weak or is the risk uncontrollable)
- Additional controls: List additional controls or strengthening existing controls to manage this risk. Each control may have different option which should be reviewed for the most cost effective. A treatment plan would be prepared for each control. This would be the implementation plan noting the tasks, cost, due date etc.

Few Points:

- In general managing your risks is done by:
  - Reducing the likelihood of a possible event occurring
  - Reducing the consequence (or impact) when a possible incident occurs.
- However this depends on a number of factors such as:
  - Nature of the risk: ie: it is not possible to manage the likelihood of a cyclone however it is possible to manage the consequence/impact.

Risk Register: The following is a template you can use.

- Information captured on the risk register varies and normally depend on the context.

Risk Information

Date Created	
Context	What is Risk Management being applied to? (I.e.: Your annual plan, specific project)
Created by	
Date: reviewed	
Date next review	

Risk Register

Risk #	Type	Risk Description and scenario	Current		Risk Rate	Effectiveness of controls	SMT (Risk Owner)	Delegated to (Risk Owner)	Due Date	Change (Risk)
			L	C						

Type / Category	Source of Risk - Select a pre-define type (or also knows as category). Refer to table below. This will assist group similar risks. (Refer to table 'Sources of Risks" - below)				
Current:	Where you are now considering controls in place. (Also referred to as the residual risk)				
Risk Rate	Refer to the Risk Matrix (i.e. Extreme, High, Medium, Low).				
Effectiveness of Controls	Strong, Moderate, Weak, Uncontrollable (Examples: Refer to Criteria Table – Controls)				
Change (Risk): Change is risk since last review	N – New Risk	↑ Increase	↓ Decrease	↔ No change	X - Closed

- For project risks you may want to include additional columns to assist you monitor the treatment plans.
- To assist you manage your risks we provided several guides/self-assessments online. These guides include information to consider including in your risk register. (Guides such as: USP events, Managing your contract risks, Money policy, All Risk policy).
- The important point is to ensure you are capturing only the relevant information to manage/monitor your risks.
- **Sources of Risk (Risk Type or Category)**
- The risk assessment considers strategic, financial, operational and hazard risks including;

Asset Type / Category		Summary description
1	**Asset Management**	Loss, damage, destruction, loss of use of own or other party's buildings, plant, equipment, stock, and intellectual property.
2	**Compliance**	Failure to comply with regulatory requirements and legal obligations, internal or external.
3	**Governance and Management**	Consequences of poor corporate governance and/or general management practices.
4	**People**	Injury to staff and other people; failure of duties of care to other parties. Human resources management practices.
5	**Environment**	Damage to the environment. Environmental management practices.
6	**Business Model / Change Management**	Impact on the business of poorly managed strategic development and change processes.
7	**Financial**	Reduced revenue and/or increased expense flows. Financial management practices.
8	**Products / Services**	Liability arising from product or service. Quality or delivery.
9	**Digital**	Impacts relating to the management and failure of technology.
10	**Research**	Innovation management and failure of private section engagement and participation, non-delivery of research project.
11	**Learning and Teaching**	Impacts relating to the quality of teaching, alignment with USP vision and mission.