

# Guideline - Risk Register

### Introduction

The Risk Management Framework is a component of the Risk and Business Management suite. The suite includes:

* Risk Management – including risk registers
* Business Continuity Plans –including business impact analysis
* Emergency Response Plans
* Health and Safety Plans

This document defines commonly used risk management terms and sets out the risk register format that Victoria has adopted. This document should be read in conjunction with our Risk Management Policy and provides a process to help us better manage and minimise the risks associated with our work.

All decisions involve risk management. Risk should be considered throughout the development and implementation of any business process or project. Risk management is a structured and systematic process which is part of business as usual (BAU). Managers need to consider the risk in delivering business, how to manage that risk effectively through implementing strategies based on the amount of risk the University considers is tolerable. This document broadly considers risk as anything that could prevent us from achieving our goals or an outcome resulting in loss.

### Definitions:

|  |  |
| --- | --- |
| Risk | Is defined as “the effect of uncertainty on objectives[[1]](#footnote-2)”.  Risk is measured in terms of likelihood and consequence. |
| Raw Risk | The risk before anything is done to mitigate or manage it, i.e. before controls are put in place. |
| Residual Risk | The risk faced after putting in place controls or mitigation actions. |

1. **Organisational Scope**

All Managers are responsible for identifying, assessing and managing the risk within their areas of control and for ensuring that appropriate risk management activities are functioning effectively.

1. **Framework Content and Guidelines**

The Risk Management Plan is made of four stages:

* Identifying and managing risks - Risk Register;
* Identifying key or priority risks – Risk Report Summary;
* Reporting and escalating risks at the appropriate time; and
* Reviewing risk in an on-going cycle.

This document provides guidance on completing a risk register and the risk report summary. Managers are required to report key risks to their managers and escalate as appropriate to SMT. This is a key component of a manager’s responsibilities. For guidance on the formal reporting cycle refer to the *Risk Management Programme: Operational Risk*.

### 4.1 Identifying and Managing Risks – Risk Registers

Risks are identified and assessed on a risk register. Appendix 3 contains a sample risk register using the University’s standard template. Copies of blank templates are available from Safety and Risk (email [safety@vuw.ac.nz](mailto:safety@vuw.ac.nz)).

**4.1.1 Identifying risks**

Risks are identified through environmental scanning (keeping ourselves updated on our operating environment), planning processes, major projects, investigating incidents (risk assessment and mitigation actions are essential elements), internal monitoring (regular audit and inspection) and throughout the change management process. Managers should identify sources of risk, their causes and their consequences.

Managers should consider all sources of and contributors to risk associated with delivery of their business. From this we can determine the effect on our objectives from uncertainty associated with these factors. Consideration should be made of factors including:

* Health & Safety
* Service delivery
* Legal and regulatory
* Finance
* Reputation
* Adverse media coverage
* Environmental impact
* Product quality
* Human Resources
* Information

**4.1.2 Assessing the effects**

Risks are assessed by considering the consequences of an event and the likelihood of the outcome occurring. The risk assessment is carried out by the manager responsible for the work area or process being assessed.

The table in Appendix 1 provides guidance for calculating risk levels.

The likelihood scale is based on the event occurring in the *next year*. This process provides information to help us decide whether the risks need to be treated and the most appropriate control.

**4.1.3 Managing risk – controls and assurance**

Victoria University has developed an integrated assurance framework to bring together mitigating practices such as the reporting framework, statutes, policies, procedures, and guidelines or physical controls that the University uses to govern its work. This approach provides clarity over any areas where there is an assurance gap, helps to avoid duplication, and focuses assurance on strategic drivers and initiatives.

Further internal controls that support the management of risk are business continuity plans, emergency response plans, health and safety plans and internal audit and academic reviews. The University’s policies are kept current and indexed by function in an accessible, well-maintained website and an internal audit reviews the effectiveness of the internal control system within the University. Independent audit is also carried out in line with our ACC workplace H&S accreditation.

Managers should implement their own assurance programme to check the risk controls in their areas and

develop a realistic actionable mitigation plan for each major risk including whether/how a risk is currently managed , such as business as usual (BAU) processes or other internal controls already in place. It is important that, where possible, mitigations dovetail with existing plans.

The impact of all mitigating actions and sources of assurance are considered before calculating the ‘residual’ risk. Therefore, theoretically, either likelihood or consequences or both likelihood and consequences of risk can be reduced. It really depends on the nature of the risk, the underlying subject matter and what specific treatment plan or controls have been identified. If a control system has been listed but is not performing as well as originally intended, then the manager’s mitigation plan will include the improvements to implementation, application or structure of the risk control in this case.

*Examples:*

1. The risk of key university systems and processes being immobilised or disrupted in the event of an earthquake.

*Control*: An effective business continuity and disaster recovery plan.

*Comment*: This does not reduce the likelihood of an earthquake occurring, but it does reduce the impact on essential operations.

1. The risk of the University not complying with key legislation.

*Control:* A robust legislative compliance framework which clearly identifies key legislation and ensures there are processes.

*Comment:* It may not however, be able to influence the impact if non-compliance was to occur.

1. The risk that VUW staff incur expenditure that is not in line with University goals.

*Control 1:* Systems that enforce segregation between purchase order creation and approval. *Comment:* This reduces the likelihood of such expenditure occurring.

*Control* 2: Systems that require “sign-off” from appropriate staff depending on the value of the transaction, e.g. delegated financial authorities.

*Commen*t: This reduces the impact, i.e. dollar value, of the risk.

*Both controls working in combination (fairly typical in most financial systems) will reduce both the likelihood and impact of the risk.*

The table in Appendix 2 provides managers with guidance on how to evaluate the effectiveness of risk controls. The controls are ranked level 1 – 3. A level 1 control is the most robust. A level 3 control is the least robust. Managers should consider also how well the control (already in place) is implemented or complied with. For example if a procedure is listed as part of the control mechanism but our audit process identifies that it is not complied with, the control is considered to be weak, therefore the manager will not reduce the assessed risk value significantly. A mitigation plan should be developed to address poor compliance.

If multiple controls are in place and a good level of compliance is verified by our audit process, then the control effectiveness is considered to be robust and the manager can reduce the residual risk.

**Appendix 3 - Risk Register**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Risks numbered for reference and mapping | Risk description | Risk Consequences | Raw Risk  1= lowest 5=highest | | | | Mitigations/controls | | Sources of Assurance | | Residual Risk (RR)  (after mitigation actions and controls) | | |
| Likelihood (L) 1-5 | Consequence (C) 1-5 | Raw Risk  (L x C) |  | |  | | L  1-5 | | Consequence  1-5 | RR  (L x C) |
| 1-Requirements | Lack of clear guidelines for project, project outcome. Not having enough deliverables or features to sustain a full year project. | Wasted learning opportunity. Impact on course grades due to lower quality project management assessments. | 2 | 5 | 10 | Early check in with client and asking for difficult end product to scale down from.  Clear list of requirements/deadlines to meet. | | Meeting with client.  Specified feature planning.  Dates for deliverables. | | 1 | | 2 | 2 |
| 2 -  Too many features | We are provided too many features to add and extend rather than a core concept which we can deliver first, then extend later. | Huge time sink working out adding and implementing features versus delivering on the project goals. | 2 | 3 | 6 | Establish clear outline with client, then seek further extension if possible. | | Meeting with client. | | 1 | | 1 | 1 |
| 3 -  Finance | Depending on what method we use for detection, it could be based in machine learning which requires extensive processing power. | Costs a lot to meet the hardware requirements the software needs to perform. | 1 | 2 | 2 | Discuss with client and research methods to reduce computational power. | | Testing. | | 1 | | 1 | 1 |
| 4 -  OSI adherence | The scope of what we need to deliver may require technologies out of our grasp, so require libraries. | These libraries might not be open source which goes against the brief of the project. | 2 | 3 | 6 | Research what technologies are available for use to use. | | OS distinction from library. | | 1 | | 1 | 1 |
| 5 -  Technical  scope | The potential of this project may require advanced image detection for motion and objects could be out of our scope. | Couldn’t deliver on the client’s wants and would have to downscale. | 1 | 3 | 3 | Spend extra time to learning new technologies. | | How we are able to apply what we have learnt. | | 1 | | 2 | 2 |
| 6 -  Dynamics of deployment | We would be first testing on a singular intersection, with just one angle. Doesn’t allow for expansion. | Our system would only work for a certain intersection and light setup. | 3 | 2 | 6 | When we are testing find and use other instances of intersections. | | Client defining where they want the system used. | | 1 | | 2 | 2 |
| 7 -  Privacy | Continual camera feed would be spying and noting down their license plates if we get to that point. | Legal issues through licensing of product. | 1 | 1 | 1 | Be cautious as to how we extend our product. | | Legal documentation. | | 1 | | 1 | 1 |

**Appendix 4 – Heat Map**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Consequence** | 5 |  | 1 |  |  |  |
| 4 |  |  |  |  |  |
| 3 |  | 2,4 |  |  |  |
| 2 |  |  | 6 |  |  |
| 1 | 7 | 3 | 5 |  |  |
|  | 1 | 2 | 3 | 4 | 5 |
| **Likelihood** | | | | | |

1. 1. AS/NZS ISO 31000:2009 – Risk management – principles and guidelines

   [↑](#footnote-ref-2)