

# Create a Risk Quick Reference Guide

## Enterprise Risk Management



JAMES COOK  
UNIVERSITY  
AUSTRALIA



# DOCUMENT CHANGE CONTROL

Issue	Date	Amended By	Change
Version 0.1	11/11/2021	Risk and Compliance Officer	Create Risk - Quick Reference Guide for Enterprise Risk Management
Version 0.2	22/11/2021	Risk and Compliance Officer	Amendments
Version 0.3	12/01/2022	Risk and Compliance Officer	Amendments
Version 1	10/03/2022	Risk and Compliance Officer	Released

## Contents

Overview .....	4
Create a New Risk.....	5
1. Establish the Context.....	6
2. Risk Assessment.....	7
a. Risk Identification .....	7
b. Risk Analysis .....	7
c. Risk Evaluation.....	8
3. Risk Treatment.....	9
4. Recording and Reporting .....	10
5. Monitoring and Review.....	11
6. Communication and Consultation .....	11
Appendices.....	12
Appendix 1 - Login to RiskWare.....	12
Appendix 2 - RiskWare Layout and Navigation .....	13
Appendix 3 - Navigation Tools and Commands.....	15
Appendix 4 - Risk Matrix.....	17

## Overview

The Enterprise Risk Register (ERM) is a module available in Riskware that allows a Risk Owner to create, manage, review and report on risks. The ERM Register has an integrated workflow capability that offers users the ability to approve, review and assign tasks to mitigate risks.

The University's Risk Management process complies with AS ISO 31000:2018 and is in line with JCU Risk and Compliance Management policies.

The risk management processes consist of a series of steps that, when undertaken in sequence, will enable the user to identify, assess, control and manage potential impacts and opportunities. The elements of the risk management process are presented in Figure 1.

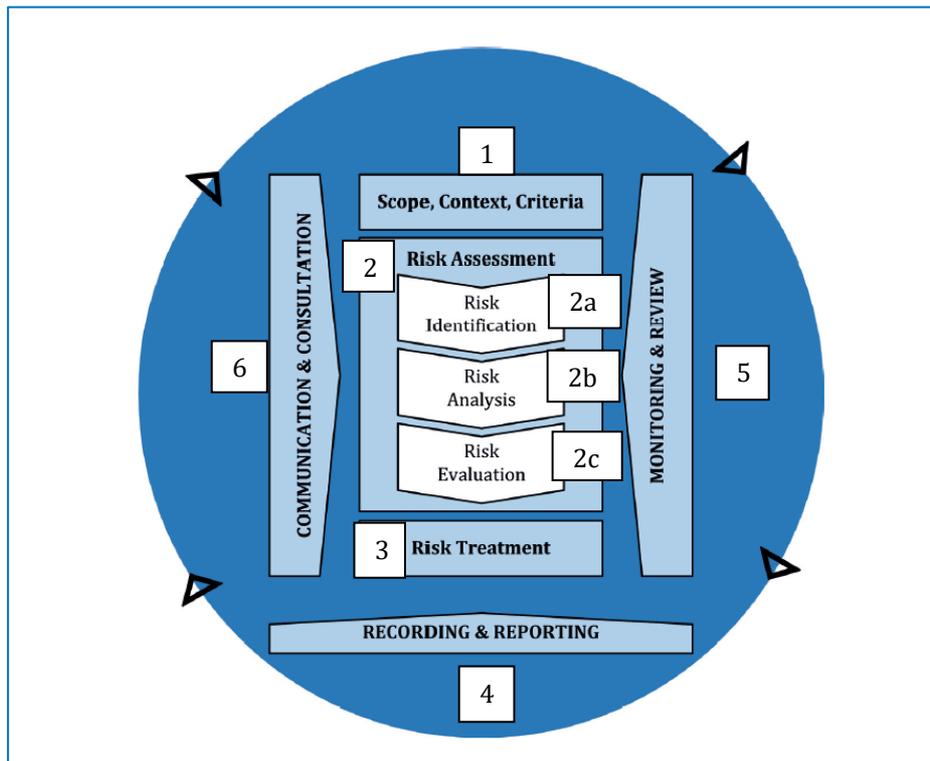


Figure 1 – Risk Management Process

Source: AS ISO 31000:2018

Under this approach, there are six key stages to the risk management process:

1. Establish context - the scope, boundaries and criteria
2. Risk Assessment - identify, analyse and evaluate risks
3. Treat Risks - implement and assess controls to address risk
4. Monitoring and review - risk reviews and audit
5. Recording and Reporting – effective governance
6. Communicate and consult - with internal and external stakeholders

The JCU Risk Management Framework applies the AS ISO 31000:2018 principles, framework and process of managing risks. As such the ERM Register in Riskware has been designed with this risk management process in mind.

The creation of a risk demonstrated in this Quick Reference Guide will focus on the first 3 stages of the process, as illustrated in Figure 2 below.

## Create a New Risk

In the Enterprise Risk Register, to create a new risk click on the 'New' icon. A Risk Assessment Form will appear.



The screenshot shows the 'Enterprise Risk Assessment' form. It is divided into several sections:

- 1** **CONTEXT**: Contains Step 1 (Classify the Risk) and Step 2 (Select one or more impacted Risk Consequence Category). Step 1 includes fields for Date Risk Identified, Risk Owner, Business Unit, Business Function, and Risk Category. Step 2 includes checkboxes for Academic, Compliance & Liability, People, Strategic, Business Disruption, Financial, Reputation, and WHS.
- 2a** **IDENTIFY**: Step 3 (Risk Description - Identify and describe the Risk) with a large text area.
- 2b** **ANALYSE**: Step 4 (Risk Source/Causal Factor) with a dropdown menu for Risk Source Category.
- 2c** **EVALUATE**: Step 5 (Existing Control(s)) with a text area, dropdowns for effectiveness and oversight, and a 'Select the person responsible' field.
- 3** **TREAT**: Step 6 (Current Risk Rating) with a 'Matrix' button; Step 7 (Risk Treatment Option) with a dropdown for Treatment Options; Step 8 (Risk Treatment Plan) with a text area; Step 9 (Who is responsible and by when?) with a dropdown; and Step 10 (Residual Risk Rating) with a 'Matrix' button.

Figure 2: Risk Assessment Form

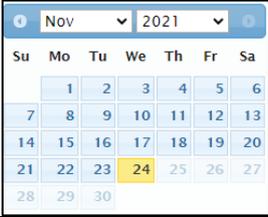
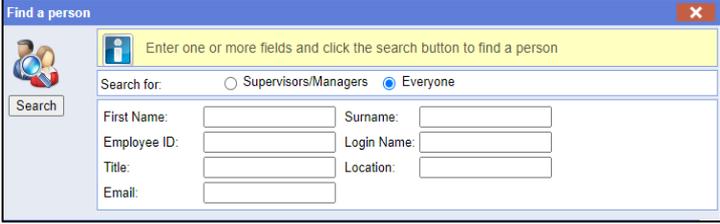
All parts denoted with a are required fields.

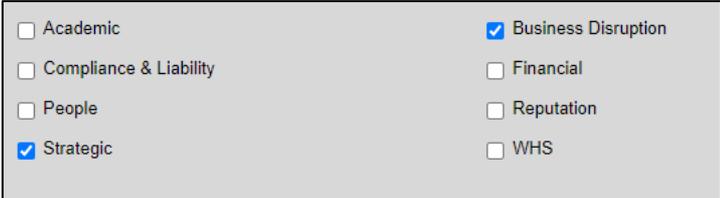
**Refer to:**  
**Appendix 1 – Login to Riskware**  
**Appendix 2 – Layout and Navigation**  
**Appendix 3 - Navigation Tools and Commands**

For more information on Risk Management processes, policies and procedures, please refer to the [JCU Risk Management Policy](#) and [Risk Management Framework and Plan](#)

## 1. Establish the Context

The context of the risk should be established from the understanding of the external and internal environment in which JCU operates and what impact such a risk may have on preventing us from meeting our strategic and business objectives.

Step 1	Establish the Context
<p>In Step 1 of the Risk Assessment form, assign a Risk Owner and select the primary affected Business Unit and Business Function. Once the Business Unit has been selected, select a primary affected Risk Category.</p>	
<p><u>Enter Date</u></p> <p>When selecting a date, any current date or a date in the past can be selected from the dropdown.</p>	
<p><u>Risk Owner</u></p> <p>Your name will appear (as default). You can also assign another Risk Owner.</p>	
<p>Select the primary affected <u>Business Unit</u> and then Select the affected <u>Business Function</u></p>	
<p>Select the primary affected <u>Risk Category</u>:</p>	

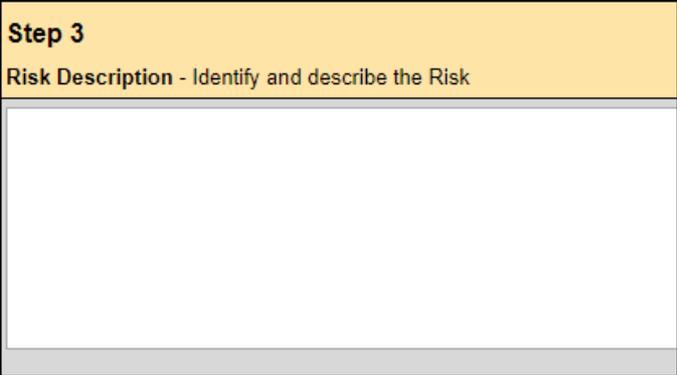
Step 2	Impacted Risk Consequence Categories
<p>In Step 2 of the Risk Assessment form select one or more <b>Impacted Risk Consequence Categories</b> should this risk occur. That is, select one or more categories that could be impacted if this risk were to materialise.</p>	
<p>Select one or more impacted <u>Risk Consequence Categories</u>.</p> <p>Selecting a risk category will enable the Current and Residual Risk Rating Matrix to perform a Risk Evaluation (Steps 6 &amp; 10)</p>	

## 2. Risk Assessment

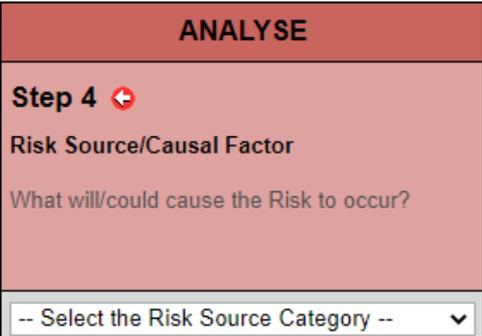
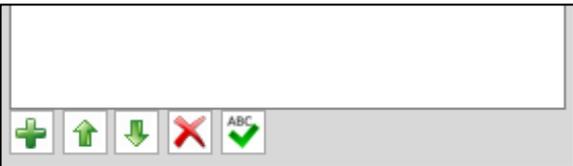
### a. Risk Identification

What are the risks that are inherent to the business objective and planned strategies?

Consider how this risk will affect the existing risk profile of the University. Be creative, but realistic in developing risk scenarios.

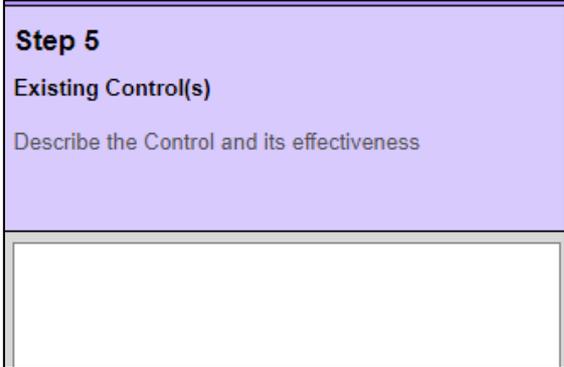
Step 3	Risk Identification
In Step 3 in the <b>Risk Description</b> textbox, identify and describe the risk.	
<p>Consider:</p> <ul style="list-style-type: none"> <li>• what can go wrong,</li> <li>• when and where, and</li> <li>• how and why.</li> </ul>	

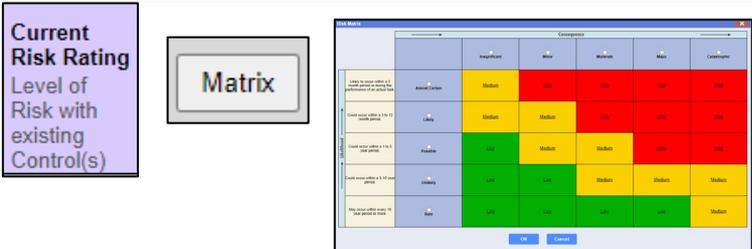
### b. Risk Analysis

Step 4	Risk Source/Casual Factor
In Step 4 of the Risk Assessment form in the <b>Risk Source/Casual Factor</b> textbox describe the reasons that would cause this risk to occur.	
<p>Select the Risk Source Category. Risk Source Categories have been categorised as: Internal and External risk sources.</p> <p>From the dropdown select one of either:</p> <ul style="list-style-type: none"> <li>• External Events</li> <li>• Internal – People, Process, Systems</li> <li>• Legal &amp; Compliance</li> </ul>	
<p>In the textbox, enter a description that clearly articulates the perceived cause of the risk by asking: “What will/could cause the risk to occur?”</p> <p>You can add multiple risk sources by clicking on the ‘Add’ icon. Move the significance of the risk source ‘Up’ or ‘Down’. ‘Cancel’ the risk source.</p> <p>Refer to Appendix 3</p>	

c. Risk Evaluation

What existing controls are in place to manage this risk or similar risks at present? How effective are these controls in managing this risk or similar risks? It is important to determine at this point, what risk controls are **currently** employed to mitigate the risk and their effectiveness.

Step 5	Existing Controls
<p>In Step 5 of the Risk Assessment form enter:  <b>Existing Controls</b> that are currently in place to manage the risk.  <b>Control Type</b> for this identified existing control.  <b>Control Effectiveness</b> rating that the risk owner can determine in consultation with relevant stakeholders.</p>	
<p>Describe the Control and its effectiveness</p>	 <p>The screenshot shows a form field with a purple header containing the text 'Step 5 Existing Control(s) Describe the Control and its effectiveness'. Below the header is a white text input area.</p>

Step 6	Current Risk Rating
<p>In Step 6 of the Risk Assessment form the effectiveness of the current controls can be assessed. This will determine the current risk rating of the risk.  <b>Note: this can be done at a later date once more information has been gathered about the risk and proposed mitigation actions.</b></p>	
<p>Control Effectiveness</p>	 <p>A dropdown menu with the text '-- How effective is the Control? --' and a downward arrow.</p>
<p>Control Effectiveness – Oversight  <b>(Complete during Risk Review)</b></p>	 <p>A dropdown menu with the text '-- Control Effectiveness: Oversight --' and a downward arrow.</p>
<p>Select the person currently responsible for managing this risk.</p>	 <p>A text input field with the placeholder text 'Select the person responsible' and a magnifying glass icon.</p>
<p>Is this a Key Control?            Select this tick box if this control is common and can be referenced from the control library in future.</p>	 <p>A checkbox labeled 'Key Control'.</p>
<p>Click on <b>Matrix</b> and determine the <b>Current Risk Rating</b> based on the <b>effectiveness of the existing controls</b>.</p> <p>Risks are measured against two key criteria:</p> <p>The <b>likelihood</b> of the event occurring.            The <b>consequence</b> or impact of an adverse event.</p> <p>Based on the likelihood and consequence click on the appropriate box and click <b>OK</b>.</p>	 <p>The image shows a 'Current Risk Rating' box with the text 'Level of Risk with existing Control(s)' and a 'Matrix' button. To the right is a screenshot of a Risk Matrix table with columns for 'Likelihood' and 'Consequence' and rows for 'High', 'Medium', and 'Low' risk levels. The cells are color-coded: High/High is Red, High/Medium is Yellow, High/Low is Green, Medium/High is Yellow, Medium/Medium is Green, Medium/Low is Green, and Low/High is Yellow, Low/Medium is Green, and Low/Low is Green.</p> <p>See Appendix 4 to view the Risk Matrix.</p> <p>Ensure Risk Consequence Categories have been selected (described in Step 2)</p>

### 3. Risk Treatment

Is the risk within the risk tolerance level?

Based on the result in Step 6 of the Risk Assessment form, **if the *current risk rating* is greater than the *organisations risk tolerance level* then you should treat the risk to reduce the level of risk to an acceptable level.**

The objective here is not necessarily to eliminate risks but rather to reduce the risk to the point where it is as low as reasonably practicable and acceptable by the organisation.

Step 7	Risk Treatment Option
In Step 7 of the Risk Assessment form, select your <b><i>Treatment Option</i></b> .	
<p>Part of the Risk Evaluation Process is to consider what course of action to take.</p> <p>This decision can lead to:</p> <ul style="list-style-type: none"> <li>• Accept the Risk, or</li> <li>• Treat the Risk</li> </ul>	<div data-bbox="619 645 1380 987"> <p><b>Step 7</b></p> <p><b>Risk Treatment Option</b></p> <p>Select your Treatment Option to mitigate/manage this risk</p> <p>-- Treatment Options --</p> </div> <div data-bbox="619 1025 858 1122"> <p>1. Treat the Risk</p> <p>2. Accept the Risk</p> </div>
Step 8	Risk Treatment Plan
In Step 8 of the Risk Assessment form, enter your <b><i>Treatment Plan</i></b> to mitigate and reduce the risk to an acceptable level.	
<p>The purpose of the risk treatment is to select and implement options for addressing risk.</p> <p>Consider:</p> <ul style="list-style-type: none"> <li>• Formulating risk treatment options most suitable</li> <li>• Planning and implementation of treatment</li> <li>• Assessing the effectiveness of that treatment</li> <li>• Deciding whether the remaining risk is acceptable</li> <li>• If not, taking further treatment</li> </ul>	<div data-bbox="619 1321 1104 1509"> <p><b>Step 8</b></p> <p><b>Risk Treatment Plan</b></p> <p>Describe your Treatment Plan to mitigate/manage the Risk</p> </div> <div data-bbox="619 1547 1104 1809"> <p>-- How effective is the Control? --</p> <p>Key Control <input type="checkbox"/></p> <p> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> </p> </div>
Step 9	Person Responsible, Due Date and the Percentage Complete

In Step 9 of the Risk Assessment form, enter the **Person Responsible**, **Due Date** and the **Percentage Complete** to ensure your **Treatment Plan** specified in Step 8 is implemented and a Task Owner is assigned.

### Step 9

Who is responsible and by when?  
Select the person and due date

### Step 10

### Residual Risk Rating

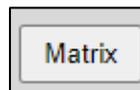
In Step 10 of the Risk Assessment form, click the **Matrix** button and determine the **Residual Level of Risk** based on **if the Treatment Plan(s) you have entered** in the above steps **were to be implemented**. Risks are measured against two key criteria:

The **likelihood** of the event occurring.  
The **consequence** or impact of an adverse event.

Based on the likelihood and consequence click on the appropriate box and click **OK**.

### Step 10

Residual Risk Rating  
Level of Risk after Treatment



See Appendix 4 for an example Risk Matrix.

Ensure Risk Consequence Categories have been selected (described in Step 2)



Once you have entered the details in the Risk Assessment Form click the **Save or Submit** button located on the toolbar.

**Note: It is only once you click on 'Submit' that a risk will become active on the risk register.**

## 4. Recording and Reporting

A number of risk management reports, graphs and charts are available for you to print and communicate risk to relevant stakeholders. Click on '**Analysis**' to access.



## 5. Monitoring and Review

Ongoing monitoring and reviews are essential to ensure that risk management plans remain relevant. Factors that may affect the likelihood and consequence of an outcome may change over time, as may the factors that affect the suitability or cost of the treatment options. It is therefore necessary to regularly repeat the risk management cycle. Periodic reviews are essential to ensure the controls you have in place to mitigate the risk are effective and the risk tolerance level is not exceeded. Refer to the '**Review a Risk**' Quick Reference Guide.

## 6. Communication and Consultation

Ensure the University is properly informed of current and emerging risks. Communicate with a wider audience to mitigating risks through the assignment of treatment plans. Also bring the risk management discussion into meetings. Regularly provide risk management reports to relevant stakeholders on how the risks are being managed.

## Appendices

### Appendix 1 - Login to RiskWare

The link to RiskWare is available on the JCU website. To access via the JCU website, you will need to do the following:

Open your Internet Browser to the JCU Homepage and click on '**Staff**'. Scroll down and select **Riskware**. Click on '**Log into Riskware**'.

	<b>Enterprise Risk Management Users will be required to provide their username and password to Log In. This is now automated using the Multi-Factor Authentication and Single Sign-On.</b>
---	--

Once successfully logged in to Riskware, on the Home Page, Click on '**Enterprise Risk Register**'.

	<a href="#">Enterprise Risk Register</a> View and manage Enterprise Risk Assessments
---	---

### Exit RiskWare

To exit always use the LOGOUT option which is located at the top right-hand side of the navigation screen.

					
 <a href="#">Home</a>	 <a href="#">My Tasks</a>	 <a href="#">Analysis</a>	 <a href="#">Feedback</a>	 <a href="#">Logout</a>	

# Appendix 2 - RiskWare Layout and Navigation

## Home Page

The Home Page features a top navigation bar with a **Global Menu** containing links for Home, My Tasks, Analysis, Maintenance, Feedback, and Logout. Below the menu, a welcome message reads "Welcome, Dimitri Dimopoulos".

The main content area is divided into three sections:

- Notification Centre:** Displays alerts such as "You have 20 Enterprise Risks in draft", "There are 24 Enterprise Risks for review", and "You have 1 Task to perform".
- Business Functions:** A list of functional areas with trend indicators: Chancellery - International, Engagement, Finance and Resources, Human and Intellectual Capital, Learning and Teaching, Organisational Effectiveness, and Physical Infrastructure.
- Heat Map (Current Risk Rating):** A 5x5 grid showing risk concentrations in various colors (red, yellow, green).

At the bottom, the **My Tools** section includes icons for: Enterprise Risk Register, Incident/Claim/Hazard Register, WHS Risk Register, Field Trip, Incident/Claim/Hazard Reporting, Analyse Data, and System Maintenance.

## Menu Explanations

### Enterprise Risk Management (ERM) Register

The Enterprise Risk Register interface includes a **Toolbar** at the top with options like Back, New, Filter, Refresh, Print, Export, and Help. The main display is a table of risks, with a **Group Risk Display** dropdown menu set to "Risk Rating - Current".

The risk table is organized into three categories: High, Medium, and Low. Each row represents a specific risk with its ID, description, owner, and current/remaining risk ratings.

Annotations highlight the **Risks** (the main data rows) and **Commands** (the icons at the end of each row used for actions like edit, delete, or refresh).

Rid	Trend	Risk Description	Risk Owner	Risk Rating		Last Review	Next Review	Commands
				Current	Residual			
<b>High</b>								
1061		JCU's ability to hire dentists could compromise its ability to consistently deliver patient services		High	High	29/07/2020	29/04/2021	[Icons]
1055		Insufficient patient numbers may affect Queensland Government WOOs and therefore possibly result in a decrease in funding.		High	High	29/07/2020	29/04/2021	[Icons]
1054		The lack of available/qualified dentists will compromise the level of student supervision required to run the clinic		High	High	29/07/2020	29/04/2021	[Icons]
1021		Loss of Key Employees		High	Medium	30/11/2020	1/09/2021	[Icons]
997		Loss of compromised service delivery due to physical infrastructure failure or degradation. Integral to student experience and competitiveness as well as supporting teaching, research and engagement activities across the University.		High	Medium	6/12/2019	6/09/2020	[Icons]
<b>Medium</b>								
1100		Negative effect of COVID on JCU Dental Business		Medium	Medium	6/07/2021	6/07/2022	[Icons]
1008		Boating and Diving Boat Yard. Theft of sonar equipment from boats in April 2021. The cost to replace was under \$10,000 and could therefore not be claimed under insurance. Future incidents may cause business disruption and impact research outcomes. There is a risk that this can occur again.		Medium	Medium	12/05/2021	12/05/2022	[Icons]
1079		JCU Dental will not be recognized as a safe and high-quality healthcare facility if it is not accredited under the National Safety and Quality Health Service (NSQHS) Standards. Qualified dentists are under a legal obligation to operate in a clinical environment that meets all of the appropriate current Australian standards and so JCU Dental must comply with NSQHS standards. The reason for NSQHS standards is provide patients the safest most appropriate clinical care as part of the Australian Charter of Healthcare Rights.		Medium	Medium	29/07/2020	29/07/2021	[Icons]
1059		The relationship between the Dental School and JCU Dental could deteriorate if alignment between dental theory and practice is not closely managed		Medium	Medium	29/07/2020	29/07/2021	[Icons]

## Global Menu

<b>Home</b>	Return to the RiskWare Home Page where you can see all of your options in the Panel.
<b>My Tasks</b>	View Incidents and Hazards that require further action.
<b>Analysis</b>	View statistical information and run reports
<b>Feedback</b>	Used to provide feedback to the RiskWare developer. Please do not use – contact JCU WHS Unit on <a href="mailto:safety@jcu.edu.au">safety@jcu.edu.au</a> for any RiskWare related issues or to provide feedback.
<b>Logout</b>	Use to log out of RiskWare

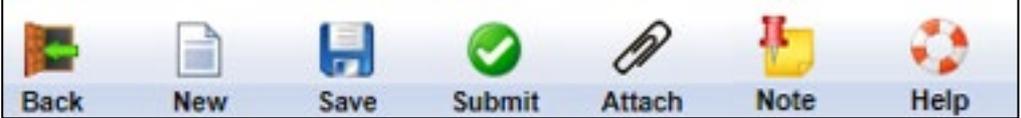
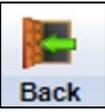
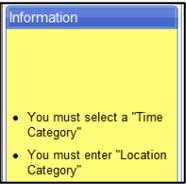
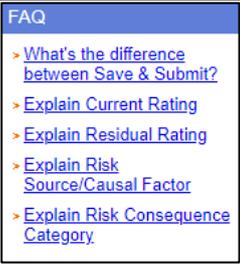
## Help

<b>Notification Centre</b>	Informs the User know which risks require action. E.g., draft, review, tasks, or any overdue risks.
----------------------------	---

## My Tools

<b>Enterprise Risk Register</b>	View and manage Enterprise Risk Assessments
<b>Other registers</b>	Used to view and manage Incidents, WHS and Field Trips
<b>Analyse Data</b>	Used for accessing statistical information and reports
<b>System Maintenance</b>	Configuration settings and system maintenance. Only accessible to System Administrators

## Appendix 3 - Navigation Tools and Commands

<p><b>Navigation Toolbar</b></p>			
	<p>Create a new Risk Assessment Form</p>		<p>Used to save as a draft in Risk Assessment</p>
	<p>Exit the Risk Assessment Form</p>		<p>Once all steps are completed the risk owner can Submit the form which will workflow to the approver</p>
	<p>Indicates a required field and must be completed</p>		<p>Attach a file or image</p>
	<p>Access to user guides (in development) Email: <a href="mailto:riskmanagement@jcu.edu.au">riskmanagement@jcu.edu.au</a> for assistance</p>		<p>Used to perform a search</p>
<p><b>General (in Risk Assessment Form)</b></p>			
	<p>Indicates a drop down list is available</p>		<p>Used to save as a draft in Risk Assessment</p>
	<p>Advises what mandatory field requires information</p>		<p>Click a question to display an answer to the FAQ</p>
	<p>Add a new textbox. This can be a Risk Source, Existing Control, or Risk Treatment Plan</p>		<p>Move the textbox up.</p>
	<p>Move the textbox down</p>		<p>Delete the textbox</p>
	<p>Check spelling</p>		<p>Add a general note or a note for a reviewer</p>

Commands			
	View Risk Assessment		Print Risk (or download as a file)
	Review Risk Assessment		View Risk Review History
	Audit Trail		Bow Tie Analysis
	Clone Risk (using similar characteristics of the risk)		

# Appendix 4 – Risk Matrix

		Consequence					
		Insignificant	Minor	Moderate	Major	Catastrophic	
Likelihood	Likely to occur within a 3 month period or during the performance of an actual task.	Almost Certain	Medium	High	High	High	High
	Could occur within a 3 to 12 month period.	Likely	Medium	Medium	High	High	High
	Could occur within a 1 to 5 year period.	Possible	Low	Medium	Medium	High	High
	Could occur within a 5-10 year period.	Unlikely	Low	Low	Medium	Medium	Medium
	May occur within every 10 year period or more.	Rare	Low	Low	Low	Low	Medium



JAMES COOK  
UNIVERSITY  
AUSTRALIA