

### **Policy Rationale**

CCAEC will adopt a formal approach to risk management to improve decision-making, performance and accountability. The goal is not to eliminate risk, but to manage the risks inevitably involved in activities to maximise opportunities and minimise negative outcomes. Risk management requires:

- + forward thinking and a proactive approach to management
- + achieving a balance between the costs of managing a risk and the anticipated benefits.

The risk management approach to be adopted is a six-step process:

- 1 Establishing the Policy Objectives and Context
- 2 Risk Identification
- 3 Risk Analysis
- 4 Risk Evaluation and Assessment
- 5 Risk Mitigation
- 6 Monitor, Manage and Review Risk Assessment

### **Policy Aims**

CCAEC will develop, maintain, review and revise, at regular intervals, procedures that provide it with a systematic view of the risks it faces in the course of its activities. The aims of CCAEC's risk management policy are to:

- Promote employee, public and customer safety
- Protect personnel, assets and intellectual property
- Encourage better quality service delivery
- Minimise loss and insurance costs
- Improve contingency planning for dealing with risks and their impact

### **Risk Management Definitions**

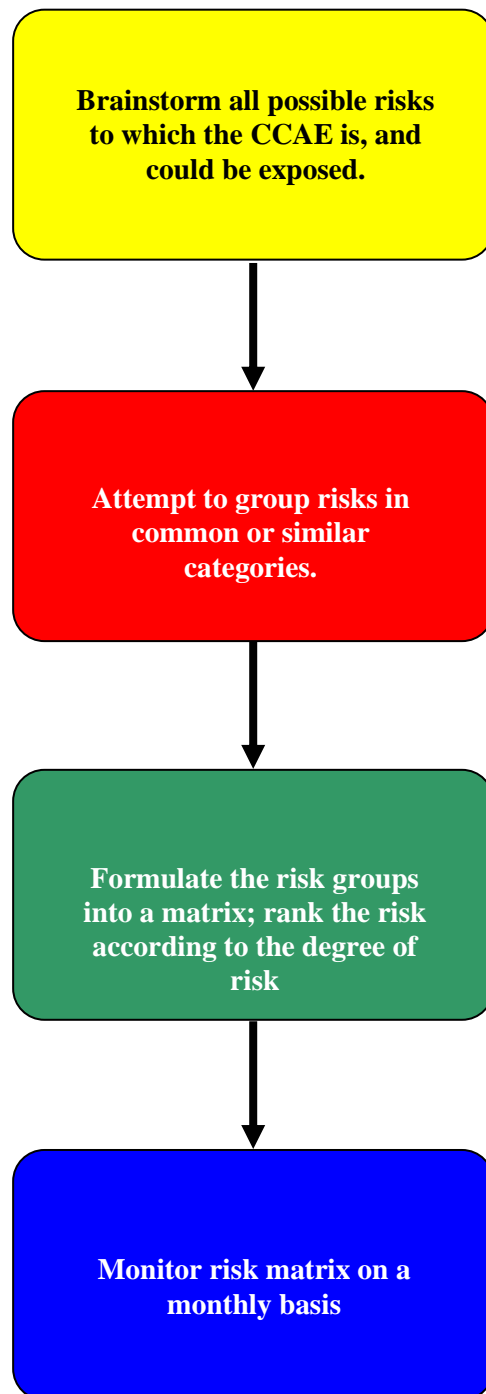
- **Risk** is the chance that an event will occur that will impact upon the CCAEC's objectives. It is measured in terms of consequence and likelihood.
- **Risk assessment** is the process used to determine risk management priorities by evaluating and comparing the level of risk against predetermined acceptable levels of risk.
- **Risk management** is the systematic application of management policies, procedures and practices to the tasks of identifying, analysing, assessing, treating and monitoring risk.
- **Accountability** involves all employees being accountable for operational risk management within the business unit or program they have been delegated. The EO is accountable for strategic risk management
- **Responsibility** involves all personnel at the CCAEC as each is responsible for the effective management of risk. All staff are responsible for identifying potential risks. Management is responsible for developing risk mitigation plans and implementing risk reduction strategies. The risk management process is integrated with other planning processes and management activities.

### **Procedures – Risk Management**

To achieve effective risk management CCAEC will:

- Continuously identify risks, develop strategies to manage the risks, monitor the effectiveness of these strategies and revise them if required.
- Ensure all staff are trained in risk management and use the Risk Analysis and Risk Management Strategy to conduct their operations and carry out their work routines.
- Ensure all risk management policy and procedures comply with relevant statutory requirements.
- See Risk Management Strategy
- See Risk Assessment Tool

## Risk Analysis and Risk Management Strategy



### Categories may include:

- Financial risk
- Contract and Legal
- Project Management
- Training Delivery

See Organisational Risk Management Systems Matrix

## Organisational Risk Management System

<u>POTENTIAL RISK</u>	<u>RISK LEVEL</u>			<u>STRATEGIES</u>	<u>ACTION 2013-15</u>
	<u>LOW</u>	<u>MEDIUM</u>	<u>HIGH</u>		
Succession Training to limit <i>It's all in my head</i> impact of Hit by a Bus [or] Walk out Door Loss of Knowledge/Skills			✓	<ul style="list-style-type: none"> <li>• Maintain 4 staff fully competent in VETtrak</li> <li>• Mentoring selected staff in technical skills</li> <li>• Multi-skilling of staff</li> </ul>	Mentoring in: <u>Statistics, TAA, Traineeship, RPL</u>  <u>Procedures on 'S' drive</u>  <u>Shared services KCLC, MHS</u>

Adoption Date: 20 June 2012

Review Date: 01/06/2015

Version Control: V1-01/07/2002

V2-30/06/03

V3-30/11/04

V4-20/08/07

V5-01/06/10

V6-01/06/12

<u>POTENTIAL RISK</u>	<u>RISK LEVEL</u>			<u>STRATEGIES</u>	<u>ACTION 2013-15</u>
	<u>LOW</u>	<u>MEDIUM</u>	<u>HIGH</u>		
<u>OHS Planning</u>			✓	<ul style="list-style-type: none"> <li>Update OHS Plan &amp; Procedures</li> <li>Communicate OHS issues to all staff at regular staff meetings</li> <li>Update BoM of OHS issues at BoM meetings and via email.</li> <li>Apply for specific purpose grants</li> <li><u>Elect site reps.</u></li> </ul>	<u>2013: Irlen: paint rooms to reduce glare; install electronic white boards; upgrade JAB rooms.</u>  <u>2014: Solar panels; car park line marking; extraction on workshop</u>  <u>2015: Roofing of CCAE building.</u>
<u>Changes to Funding Sources</u>			✓	<ul style="list-style-type: none"> <li>Develop multiple funding sources: HESG, ACFE, DHS, JSA, FFS.</li> <li>Adjust scope to provide new opportunities.</li> <li>Engage contract basis rather than casual or permanent employees.</li> <li>Tender for Government programs</li> <li>Seek co-operative training packages with indigenous RTOs and organisations.</li> <li>Seek employment programs with JSA's</li> </ul>	<u>2013: Update CHC programs; Review VCAL CGEA operations</u>  <u>2014: Initiate new CGEA / ACFE programs; Seek SVTS programs for gap year; get Transition Edu'n on scope.</u>  <u>2015: Transition Education to be used with MHS and CLR</u>
<u>IT systems and use in Admin + Training and Education programs</u>			✓	<ul style="list-style-type: none"> <li>Review IT equipment acquisition: Windows 7 + 8 Operating systems, File server, Laptops and Desktop Computers</li> <li>Maintain 2 classrooms of desktop computers</li> <li>Maintain 2 x 14 unit laptop trolleys</li> <li>Maintain 5 electronic whiteboards and 4 flat screen TV with internet connection</li> </ul>	<u>2013: Upgrade phone system and message service; upgrade laptop trolleys with recharge+printers</u>  <u>2014: Upgrade to Windows 8; Buy tablets / ipads instead of laptops</u>  <u>2015: Review file server/archive needs.</u>
<u>Lack of adequate IT security</u>			✓	<ul style="list-style-type: none"> <li>Seek funding for IT systems, maintenance and development including security</li> <li>Train staff in IT</li> <li>Seek student who can be employed as IT Trainee</li> </ul>	<u>2013: Maintain IT Trainee or IT support role</u>  <u>2014: Staff Member trained to IT-CIII level</u>  <u>2015: Investigate use of Password system for students / staff</u>

Adoption Date: 20 June 2012

Review Date: 01/06/2015

Version Control: V1-01/07/2002

V2-30/06/03

V3-30/11/04

V4-20/08/07

V5-01/06/10

V6-01/06/12

<u>POTENTIAL RISK</u>	<u>RISK LEVEL</u>			<u>STRATEGIES</u>	<u>ACTION 2013-15</u>
	<u>LOW</u>	<u>MEDIUM</u>	<u>HIGH</u>		
<u>VETTrak and MYOB aged receivables do not reconcile resulting in Bad Debt write-offs.</u>			✓	<ul style="list-style-type: none"> <li>Maintain contracted Finance Officer.</li> <li>Hire one staff member with VETtrak + MYOB to transfer VETtrak invoice and payment data to MYOB</li> </ul>	<u>2013-15: Implement the strategies to help reconciliation between VETtrak and MYOB on aged receivables.</u>
<u>Update Strategic Financial Management Planning</u>		✓		<ul style="list-style-type: none"> <li>Maintain insurances</li> <li>Improved financial management information e.g. monthly cash flow statements, program budgets, organisational financial reports</li> <li>Conduct annual review of strategic &amp; program with 3 year outlook</li> </ul>	<u>2013-15 Finance Officer develop year to date finance reports</u>  <u>Manager develop detailed annual budget and 3 year projection.</u>  <u>Strategic plan expenses built into budgets.</u>
<u>Training alliance</u>		✓		<ul style="list-style-type: none"> <li>Seek training alliance with another RTO or JSA outside Echuca</li> </ul>	<u>2013-15 seek relationship with MHS or CLR for delivery outside the Echuca area</u>
<u>Our competitors try to take OUR BUSINESS</u>		✓		<ul style="list-style-type: none"> <li>Ensure excellence in service delivery</li> <li>Awareness of competitor strengths &amp; weaknesses</li> <li>Be clear about our core business</li> <li>Build strong relationships with strategic partners</li> </ul>	<u>Be pro-active with continuous improvement</u>  <u>Focus on Cert I to Cert III outcomes where possible</u>  <u>Seek business input to programs get staff to note.</u>
<u>Board develop its governance skills</u>		✓		<ul style="list-style-type: none"> <li>Identify governance framework model</li> <li>Develop governance policies and procedures</li> <li>Review model</li> <li>Compliance with legal and contractual requirements</li> </ul>	<u>Seek new members with management skill</u>  <u>Seek new members with indigenous skills</u>  <u>Seek members from alliance organisations</u>
<u>Human resource management</u>		✓		<ul style="list-style-type: none"> <li>Develop, implement and disseminate appropriate policies and procedures</li> </ul>	<u>2013 indigenous liaison officer and new IT staff</u>  <u>2014-15 New Eng/Maths staff</u>
<u>Litigation</u>		✓		<ul style="list-style-type: none"> <li>Maintain adequate insurances cover</li> </ul>	<u>Review annually</u>

Adoption Date: 20 June 2012

Review Date: 01/06/2015

Version Control: V1-01/07/2002

V2-30/06/03

V3-30/11/04

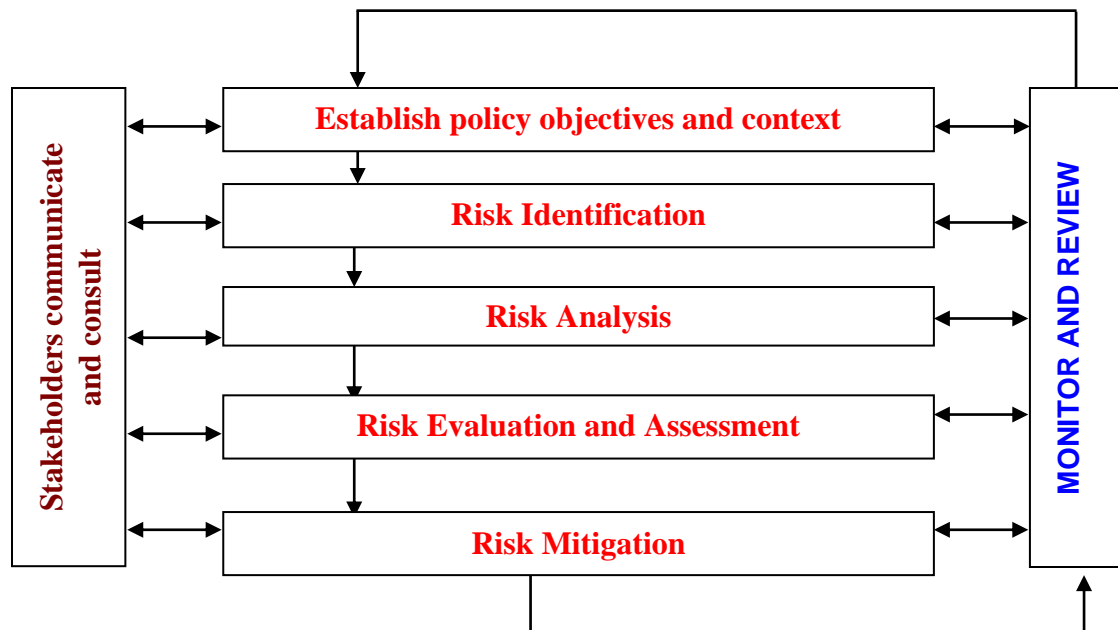
V4-20/08/07

V5-01/06/10

V6-01/06/12

## Objectives of Risk Management Procedures

- Risk Management Plans for packages focus on top-down strategic risks of the whole package instead of bottom-up risks associated with the delivery of single policy measures.
- The following diagram provides an overview of the risk management process.



## 6 Step Risk Management Procedures

### Step 1 – Establish policy objectives and environment

The risk environment relates to views of key stakeholders. Where stakeholders can exert significant influence on the achievement of policy objectives, agencies should undertake a stakeholder analysis. The communications strategy should contain the strategies for engaging with stakeholders and managing stakeholder issues.

### Step 2 – Risk Identification

A detailed identification of risks takes into account managing the implementation and delivery of policy. Some risks may be identified as resources, contracting and procurement, stakeholder engagement, quality assurance:

- lack of definition of the policy objectives and deliverables (unclear objectives/scope)
- restrictive time frames
- availability of resources – people, skills, equipment
- developing infrastructure
- lack of in-house capacity.
- Timing
- Financial
- Contractual
- Scope definition
- Related projects
- Safety
- Quality
- Resources
- Communications
- Commercial
- Organisational
- Cultural
- Technical

Agencies may find it useful to group risks into primary (highest level) risks (no more than 5) and secondary (next level down) risks. It is essential that there be documentation of the relevant risk factors that can be shared with others as required (see [Template A](#), Attachment 1).

Adoption Date: 20 June 2012

Review Date: 01/06/2015

Version Control: V1-01/07/2002

V2-30/06/03

V3-30/11/04

V4-20/08/07

V5-01/06/10

V6-01/06/12

### Step 3 – Risk Analysis

Assess likelihood of risk occurrence and potential impact (consequence). This will provide the basis for evaluating those risks that require attention. The following table provides guidance on analysing risk, likelihood / consequence:

<b>Risk Level:</b>	E	Extreme risk	Detailed action/plan required
	H	High risk	Needs senior management attention
	M	Moderate risk	Specify management responsibility
	L	Low risk	Managed by routine procedures
<b>Likelihood:</b>	A	Almost certain	Expected in most circumstances
	B	Likely	Will probably occur in most circumstances
	C	Possible	Could occur at some time
	D	Unlikely	Not expected to occur
	E	Rare	Exceptional circumstances only
<b>Consequence:</b>	5	Severe	Would stop achievement of functional goals / objectives
	4	Major	Would threaten or functional goals / objectives
	3	Moderate	Necessitating significant adjustment to overall function
	2	Minor	Would threaten an element of the function
	1	Insignificant	Lower consequence

Qualitative analysis may result in an assessment of probability of occurrence (likelihood) of rare, unlikely, possible, likely or almost certain. The consequence of a risk occurring should be rated as insignificant, minor, moderate, major or severe. An analysis can be informed through a range of processes:

- interviews with key stakeholders
- brainstorming sessions with key stakeholders
- personal experience
- review of corporate memory or policy precedents.

### Qualitative Risk Analysis Matrix

Likelihood	Consequences				
	Insignificant	Minor	Moderate	Major	Severe
Almost certain	M	H	H	E	E
Likely	M	M	H	H	E
Possible	L	M	M	H	E
Unlikely	L	M	M	M	H
Rare	L	L	M	M	H

For each risk factor use qualitative analysis to assess how the project would be affected should the risk situation actually occur. This assessment needs, as a minimum, to consider the impact on:

- time
- cost
- quality
- stakeholder perception.

Adoption Date: 20 June 2012

Review Date: 01/06/2015

Version Control: V1-01/07/2002

V2-30/06/03

V3-30/11/04

V4-20/08/07

V5-01/06/10

V6-01/06/12

#### **Step 4 – Risk Evaluation and Assessment**

To complete risk analysis, estimates of likelihood and consequence need to be considered in context of existing risk control measures. Assess the effectiveness of current risk controls or management strategies for each risk:

- when is the risk situation likely to occur?
- what are the possible courses of action available if it does occur?
- what pre-planning can be undertaken ahead of the risk occurring?
- is it worthwhile developing a contingency plan to address this risk?

Once each risk has been re-assessed in light of current controls or management strategies, mapping re-assessed risks onto a matrix as above will assist in determining whether risks should be prioritised for further action.

The revised likelihood and impact (consequence) can be used to prioritise risks according to those that are likely to require further action or treatment. As a minimum, all those ranked as 'E' extreme, or 'H' high will need further consideration and treatment in order to mitigate either likelihood, consequence or both.

#### **Step 5 – Risk Mitigation**

Once risks have been assessed and prioritised, agencies need to determine a strategy for the mitigation of each risk. In broad terms, a decision should be made either to:

- avoid or reduce the risk through application of alternative approaches to achieving the objective, or through changes to the scope, schedule, quality, budget or resource requirements; or
- transfer the risk through the use of contracts and internal agreements (to someone better able to manage it) noting that management of the risk remains the responsibility of the agency (or agencies in the case of a package of measures) accountable for the implementation of the measure/package of measures; or
- accept the risk and develop contingency plans (as required) to minimise the impact should the risk eventuate – suitable for a low likelihood risk with a potentially catastrophic impact.

#### **Step 6 – Regularly Monitor, Manage and Review Risk Assessment**

Responsibility for monitoring and management of each risk should be agreed or assigned. A single area should be given primary responsibility and this will vary between agencies but should be the person or organisation that has most control over the risk factor. For example, schedule risk might be monitored by the project manager but financial risk will be best monitored and controlled by the financial manager.

The high level reporting and accountability processes for risk management should also be reflected in the governance arrangements documented in the quality assurance section of the Implementation Plan.

In addition to monitoring and management, risks should be routinely reviewed to identify emerging risks and those that are no longer relevant. Review points can be milestone based, periodic (eg. daily, weekly, monthly), deliverable based, or in accordance with standard operating procedures. Risk factors should be listed for discussion at periodic progress meetings.

Risk management systems and actual documentation will vary between agencies but it is vital to ensure risk management plans remain current and relevant as possible to the implementation of the measures. Throughout the course of implementation, risk identification should continue to occur to take account of changing circumstances. For example, risk should be reviewed:

- prior to the release of tender documentation
- prior to formal approval to proceed to implementation
- and in conjunction with periodic reporting.

The review is best undertaken in a group environment. Review and confirm the risks identified in the current risk assessment. Identify other risks that may have arisen as a consequence of:

- changing circumstances and new developments
- further refinement of project planning
- changes to the scope of the project
- discussions/negotiations with the client/stakeholder.

As before, assess the probability of occurrence of each of the new risk factors identified. Delete risk factors that are no longer relevant. Every new risk factor should be analysed and evaluated (see steps 3-5).

**Adoption Date:** 20 June 2012

**Review Date:** 01/06/2015

**Version Control:** V1-01/07/2002

V2-30/06/03

V3-30/11/04

V4-20/08/07

V5-01/06/10

V6-01/06/12

## Risk Management Plan – Template A

### OVERVIEW OF KEY RISKS

List the key risks associated with implementation and delivery of the policy, grouped by phase and/or activity (outlined in the scope section of the Implementation Plan), on the Risk Identification form at Attachment 1. Include an explanation of the risk, its source and potential impact.

This list should be prepared in conjunction with the various sections of the Implementation Plan and the key risks relating to these sections (ie, work breakdown, funding, stakeholder engagement, resources, contracts and procurement, and quality assurance) should be included.

### RISK ASSESSMENT

Using the Risk Analysis Matrix in the risk management section of the Guide, plot the consequence and likelihood of an occurrence of each of the risks listed above. Assess, prioritise and document the level of risk associated with each using the Qualitative Risk Analysis Matrix.

### STRATEGIES FOR TREATMENT OF KEY RISKS

In order of risk priority, summarise the strategies that will be used to mitigate the risks. Strategies may include methods to avoid the risk or transfer it (ie, through outsourcing). If the risk is to be accepted, document the strategies that will be used to manage the risk. These may include the use of monitoring mechanisms, communication campaigns or leading edge technology. Where appropriate refer to contingency plan(s) described below.

For each risk, specify how frequently the risk will be reviewed and who is responsible for monitoring.

Document these strategies.

### OVERALL ASSESSMENT OF PROJECT RISK

Based on the assessment of key risks to implementation and delivery, and taking into account the treatments described above, provide an assessment of the overall risk to the project (low, moderate, high or extreme). Where possible also summarise this for each of the phases of the project.

### CONTINGENCY PLANS

Where relevant, contingency plans should be developed that will enable the effective management of the project (to meet its objectives) in the eventuality that any of the identified key risks occur. Briefly summarise contingency plans for relevant risk factors.

#### **Evaluation**

This policy will be reviewed bi-annually and as part of the CCAE's strategic planning and review process and as required by developments in relevant legislation or ACE requirements.

Adoption Date: 20 June 2012

Review Date: 01/06/2015

Version Control: V1-01/07/2002

V2-30/06/03

V3-30/11/04

V4-20/08/07

V5-01/06/10

V6-01/06/12