Department of
Education

RISK AND BUSINESS CONTINUITY MANAGEMENT

EFFECTIVE: 18 MAY 2010

VERSION: 1.6 FINAL

Last updated date: 18 March 2021

CONTENTS

1 POLICY STATEMENT

The Department of Education (the Department) manages risks that threaten to adversely impact upon employees, students, resources or the Western Australian school community. Risk and business continuity management is evidenced by integrating risk identification, risk management and consistent reporting into everyday operations.

2 BACKGROUND

The mission of the Department is to provide world class education and training to meet the needs of individuals, the community and the economy of Western Australia. The adoption of risk management and business continuity planning through a framework of systemic identification, assessment and management of all risks is integral to the successful achievement of this goal.

In addition, the following directives provide the impetus to embrace this initiative:

- *Treasurer's Instruction TI 825* which states:
  The accountable authority shall ensure that:
  - *i. there are procedures in place for the periodic assessment, identification, and treatment of risks inherent in the operations of the agency;*
  - *ii. suitable risk management policies and practices are developed;*
  - *iii. an appropriate level of security is maintained over money, public and other property of or under control of the agency, including information held and intellectual property developed and controlled by the agency; and*
  - *iv. these procedures, policies and practices are documented in the financial management manual or other relevant policy manuals.*

The objectives of risk management and business continuity planning are to:

- protect students, staff and stakeholders from adverse incidents;
- reduce risk exposure;
- mitigate and control loss;
- agree on a level of acceptable risk;
- ensure the ongoing capacity of the Department to achieve its objectives, and to perform its functions of providing quality service;
- reduce the costs of risk; and
- protect the Department and its stakeholders from loss.

This document provides policy and guidance in identifying, assessing, recording and treating risks that could impact upon the Department and as appropriate, policy and guidance in the development of business continuity planning.

3 SCOPE

This policy applies to all Department employees.

4 PROCEDURES

4.1 DIRECTOR GENERAL

The Director General shall ensure the management of risk and business continuity management throughout the Department.

4.2 LINE MANAGERS

4.2.1 RISK MANAGEMENT

Line managers will:

- identify and assess risks;
- develop treatment plans;
- monitor and record risks within the risk management system; and
- communicate risks to staff, as appropriate.

Guidelines

See Appendix A – Establishing, identifying and assessing risks.

See Appendix B – Sample risk identification worksheet.

See Appendix C – Risk reference tables.

Risk information is contained and mantained within the Department's risk management system.

4.2.2 BUSINESS CONTINUITY MANAGEMENT

Line managers will, as appropriate:

- conduct a Business Impact Analysis that identifies the maximum acceptable outage which lead to critical functions needing to be reinstated following a major incident;
- document the Business Impact Analysis in a Business Continuity Management Plan;
- review the Business Impact Analysis at least every 12 months;
- review and update the Business Continuity Management Plan at least every 12 months;
- conduct exercises on a regular basis to test or validate the plans; and
- draft the Business Continuity Management Plan that, includes:
    - strategies; requirements and procedures for continuity of critical functions; and
    - all resource requirements to support the continuity of identified functions.

Guidelines

The Department's business continuity strategies and plans should be based on the following parameters:

- *A major incident that will render any one of the Department's facilities, including premises and IT services to be inaccessible or unusable for a prolonged period.*
- *Access will not be possible within a one kilometre radius from the affected site.*
- *Public transportation and utilities (power, telecommunications and water) around the vicinity of the incident are cut or severely hampered.*
- *Alternate personnel need to be identified as backups for key positions and generally, staff will be available to execute the Business Continuity Management Plans.*

- *Alternate data centres and recovery sites, if required, are not on the same power grid and telecommunications exchange as the primary data centre / business office buildings and are located at a reasonable distance away from each other.*

For further information, see Appendix D - Business continuity management process.

Principals would be required to develop Business Continuity Management Plans in circumstances where their continuity of operations is not covered by other department processes.

4.2.3 RECORD KEEPING

Line managers will maintain the following documentation:

- individual risk reviews;
- treatment action plans; and
- Business Continuity Management Plans, as appropriate.

Guidelines
Records are maintained for audit purposes.

4.3 ALL EMPLOYEES

All employees will:

- practice risk mitigation; and
- inform their line manager of potential risks.

Guidelines
For guidelines on identifying potential risks, see Appendix A - Establishing, identifying and assessing risks.

5 RELATED DOCUMENTS

5.1 RELEVANT LEGISLATION OR AUTHORITY

Australian Standard ISO 31000:2018
Risk Management- Guidelines
Public Sector Management Act 1994 (WA)
School Education Act 1999 (WA)
School Education Regulations 2000 (WA)
Treasurer's Instruction 825 Risk Management and Security

6 DEFINITIONS

ACCEPTABLE RISK

An acceptable tolerance level, based on the level of risk after evaluating existing controls.

BUSINESS CONTINUITY MANAGEMENT

A process to ensure the timely resumption and delivery of essential business activities in the event of a major disruption by maintaining the key business resources required to support delivery of those services.

BUSINESS IMPACT ANALYSIS

The process of assessing the potential consequences to an organisation of an outage to its key business activities over varying periods of time, and prioritising the timeframes in which these activities must be resumed following a disruptive event.

CAUSE

A source of potential harm or situation with a potential to cause loss. This is also referred to as a hazard.

CONSEQUENCE

The outcome of an event or situation; being a loss, injury, disadvantage or gain. The consequence criteria scale is graduated in five levels from 'insignificant' through to 'catastrophic' measured against the following categories of context:

- student achievement targets;
- safety of people;
- financial loss;
- reputation and image to the Department and schools;
- operational efficiency and governance; and
- service interruption.

A risk may be connected to one or more of the above categories.

CONTROL RATING

A qualitative, common sense measure of the adequacy of controls in addressing a risk.

EMPLOYEE

Any person who is currently employed under the *School Education Act 1999* or the *Public Sector Management Act 1994*.

LIKELIHOOD

A description of probability and frequency. The likelihood criteria scale contains five levels from 'rare' to 'almost certain'. The likelihood assessment is the likelihood of the risk occurring with the existing controls in place and with the level of consequence identified.

LINE MANAGER

An employee responsible for a discrete area. A principal is considered a line manager.

RISK

The chance of something happening that will have an impact on objectives. It is measured in terms of consequences and likelihood.

RISK ASSESSMENT

The process used to determine management priorities by evaluating and comparing the level of risk against predetermined standards.

RISK CONTROL

A procedure, system, activity, policy or process that reduces the likelihood and/or consequences of a risk. A risk may have more than one control and a control may address more than one risk.

RISK IDENTIFICATION

The process of determining what can happen, why and how.

RISK MANAGEMENT

Risk management is the culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.

RISK REVIEW

A periodic assessment of risks to determine the continuing suitability, adequacy and effectiveness of controls and treatment to achieve the established objectives.

RISK TREATMENT

A process to modify or manage a risk. Any future or proposed controls, that may be planned but are not currently in place, are considered treatments. Once a treatment is implemented, it becomes a control or modifies existing controls.

7 CONTACT INFORMATION

Policy manager: Director Risk and Assurance

Policy contact officer: Program Manager, Risk
T: (08) 9264 0094

APPENDIX A ESTABLISHING, IDENTIFYING AND ASSESSING RISKS

Risk management involves the identification, evaluation, treatment and ongoing monitoring of a broad range of risks associated with all strategic, operational and project activities.

A.1 CONTEXT

For each individual risk assessment exercise it is important to:

- Set the parameters – what is the specific subject of the assessment?
- Identify the essential stakeholders who need to be involved.
- Ensure all participants are clear about the purpose of the assessment.

A.2 KEY ACTIVITY

Identify the key services/activities for your business unit. For example, processing payments on the Oracle system (see Appendix B).

A.3 CRITICAL SUCCESS FACTORS (CSF)

For each of your key business activities, determine what elements are essential to ensure successful outcome/s. For example, to process payments on the Oracle system, the following is needed:

- trained staff to match orders to invoices; and
- a working system.

A.4 RISK IDENTIFICATION

Write down the possible risks associated with each of your key activities' Critical Success Factors (CSF).

Look at your risks in terms of what can go wrong in relation to the specified CSF. Identify what will cause that risk to occur.

Please note: Some activities may have many associated risks. Each risk should be treated separately and given its own risk rating. For example,

- **Activity** - providing advice to client.
- **CSF** - accuracy of information.
- **Risk** - incomplete or inaccurate information.
- **Cause** - lack of trained staff.

A.5 EXISTING RISK CONTROLS

At the time of the risk assessment identify what control measures are currently in place that reduce the likelihood and/or consequences of the risk. For example, relevant Department policies can be identified as existing controls.

A.6 CONTROL RATING

Rate your controls in terms of are you doing what is reasonable under the circumstances to prevent or minimise the risk, i.e. Excellent, Adequate or Inadequate.

A.7 CONSEQUENCE

For each of your risks, what is the consequence if it does go wrong? The consequence may be financial, time and people costs or a combination of all three.

Following the same example (Appendix B) in regards to processing of payments in the Oracle system, the risk of 'lack of trained staff' can affect 'Operational Efficiency' (see Appendix C.2 Consequence Table) and can be rated as Minor **(Level 2)** 'Inconvenient delays'.

A.8 LIKELIHOOD

For each of your risks determine how likely it is that the risk will occur in your business unit. For example, lack of trained staff may be rated as Almost Certain **(Level 5)** – the event is expected to occur in most circumstances and is likely to happen more than once a year (see Appendix C.3 Likelihood Table).

A.9 RATING OF RISK

To determine risk rating, multiply the values in the Consequence and Likelihood columns.

In the same example, the Consequence of the risk was rated as a **Level 2** and Likelihood of the risk was rated as a **Level 5**. Multiplying 5 x 2, results in the rating of a **Level 10**. Therefore, the risk rating is Moderate (**Level 10**) (see Appendix C.4 Risk Rating Table).

A.10 CATEGORY OF CONSEQUENCE

For each risk, select the relevant consequence category (see Appendix C.2). In relation to the same example, the Category of Consequence is Operational Efficiency and Governance.

A.11 RISK ACCEPTANCE

Ultimately, the process gets you to a point of deciding whether the risk is acceptable or requires further action.

Risks will always occur in any business environment. This process is not about removing risks, rather we aim to manage the risk to an acceptable level.

In our example, the risk was rated a **Level 10**. The Risk Acceptance Table (see Appendix C.5) states that such a risk requires 'Urgent Management Attention' and may only be accepted by Senior Management when the existing controls are rated as 'Excellent'.

A.12 RESPONSIBLE OFFICER

Enter the name or position of the person who is responsible for ensuring the key activity is successfully completed.

A.13 RISK TREATMENT

Risk treatment involves identifying a range of options to reduce the consequences and/or likelihood of a risk, or improve the controls ratings, evaluating those options, preparing treatment plans and implementing them.

APPENDIX B SAMPLE RISK IDENTIFICATION WORKSHEET

DIRECTORATE/REGION											
BUSINESS UNIT/ SCHOOL											
KEY ACTIVITY	CRITICAL SUCCESS FACTORS	DESCRIPTION OF RISK	EXISTING RISK CONTROLS	CONTROL RATING	RATING OF RISK CONSEQUENCE (C) LIKELIHOOD (L)			CATEGORY OF CONSEQUENCE	RISK ACCEPTANCE	RESPONSIBLE OFFICER	RISK TREATMENTS
Describe key activity	What elements are needed to achieve these key activities	Description of risk associated with disruption to key activity		Excellent, Adequate, Inadequate	C	L	Rating	Business Continuity Management Plan required if category is severe interruption to services	Yes/No	Refer to Risk Acceptance Table	
Process payments in Oracle	***1. Trained staff to match orders to invoices***	***Lack of trained staff***			2	5	***10***				
		Lack of training program			2	2	***4***				
	2. Working system	***System availability***			3	2	***6***				
		Appropriate system access			4	2	***8***				
Helpdesk Service	***3. Helpdesk Delivery***	***Network availability***			4	4	***16***				
		Helpdesk application availability			4	3	***12***				

APPENDIX C RISK REFERENCE TABLES

C.1 CONTROL RATING TABLE

LEVEL	DESCRIPTOR	FORSEEABLE	EXAMPLE DESCRIPTION
E	**Excellent**	More than what a reasonable person would be expected to do in the circumstances.	Controls fully in place and require only ongoing maintenance and monitoring. Protection systems are continuously reviewed and procedures are regularly tested.
A	**Adequate**	Only what a reasonable person would be expected to do in the circumstances.	Being addressed reasonably. Protection systems are in place and procedures exist for given circumstances. Periodic review.
I	**Inadequate**	Less than what a reasonable person would be expected to do in the circumstances.	Little to no action being taken. No protection systems exist or they have not been reviewed for some time. No formalised procedures.

C.2 CONSEQUENCE TABLE

INDICATIVE EXAMPLES									
LEVEL	**RANK**	**STUDENT ACHIEVEMENT TARGETS**	**SAFETY OF PEOPLE** (including psychological)	**FINANCIAL LOSS**		**REPUTATION & IMAGE** (Including industry and community expectations)	**OPERATIONAL EFFICIENCY & GOVERNANCE**	**SERVICE INTERRUPTION**	
				Area of budget	**Monetary impact**			**Central Services/ Regional Education Offices**	**Schools**
1	Insignificant	< 5% variation	No injuries	.025% of budget	Up to $50,000	Unsubstantiated, suggested improvements, contained within the school, district or central office, no news item. Manager / School teacher involvement.	Little impact	Less than 2 days	1 class / unit
2	Minor	5 - 10% variation	First aid treatment	.15% of budget	$50,001 and up to $250,000	Substantiated, low impact, local press news item. Manager / School teacher involvement.	Inconvenient delays	3-6 days	1 year level / course
3	Moderate	10 - 25% variation	Medical treatment required	2% of budget	$250,001 and up to $3 million	Substantiated, public embarrassment, multiple news reports, state press news items. Senior management /Principal involvement.	Delays in achieving major outcomes	1-2 weeks	1 school/ campus
4	Major	25 - 50% variation	Death or extensive injuries including psychological	6% of budget	$3 000 001 and up to $10 million	Substantiated, public embarrassment, high impact, national news profile, third party actions, public ministerial involvement, political embarrassment. Director General/ Director of Education involvement.	Non-achievement of major outcomes	2 weeks to 1 month	1 district/ college
5	Catastrophic	> 50% variation	Multiple deaths or severe permanent disablements including psychological	More than 6% of budget	$10 000 001 and above	Substantiated, public embarrassment, high widespread multiple national/ international news profile, third party actions, public, ministerial involvement, Government censure.	Non-achievement of major deliverables	More than 1 month	All schools

C.3 LIKELIHOOD TABLE

LEVEL	DESCRIPTOR	EXAMPLE DETAIL DESCRIPTION	FREQUENCY
1	Rare	The event may occur only in exceptional circumstances	Once in 10 years
2	Unlikely	The event could occur at some time	At least once in 5 years
3	Moderate	The event should occur at some time	At least once in 3 years
4	Likely	The event will probably occur in most circumstances	At least once per year
5	Almost certain	The event is expected to occur in most circumstances	More than once per year

C.4 RISK RATING TABLE

CONSEQUENCE		LIKELIHOOD				
		1	2	3	4	5
		Rare	Unlikely	Moderate	Likely	Almost Certain
1	Insignificant	1	2	3	4	5
2	Minor	2	4	6	8	10
3	Moderate	3	6	9	12	15
4	Major	4	8	12	16	20
5	Catastrophic	5	10	15	20	25

RISK RATING
Major
Moderate
Minor

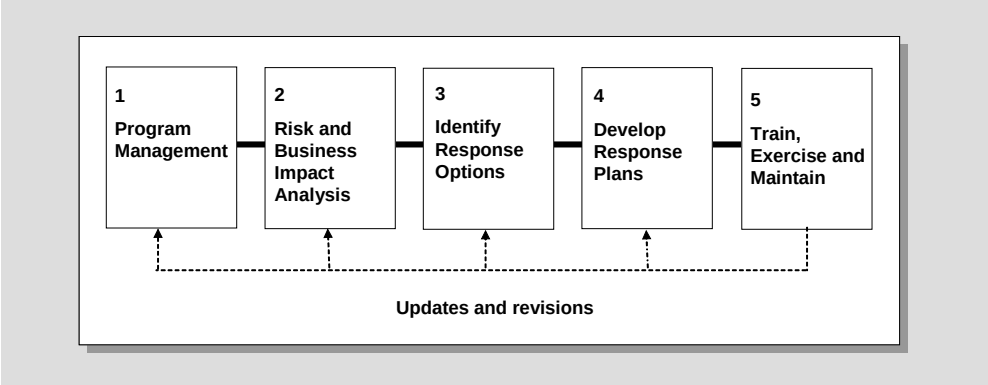
C.5 RISK ACCEPTANCE TABLE

LEVEL OF RISK	CRITERIA OF RISK MANAGEMENT		WHO IS RESPONSIBLE (i.e. person with authority to accept the risk.)
1 – 3	Acceptable	Acceptable with adequate controls	Management
4 – 5	Monitor	Acceptable with adequate controls	Management
6 – 9	Management control required	Acceptable with adequate controls	Senior Management
10 - 14	Urgent management attention	Acceptable with excellent controls	Senior Management
15 - 25	Unacceptable	Only acceptable with excellent controls	Director General

APPENDIX D BUSINESS CONTINUITY MANAGEMENT PROCESS

Business continuity management (BCM) is an integral component of risk management. Business continuity management addresses major risk events with the potential to significantly impact upon the ability to deliver critical services. It positions the Department to respond to any eventualities including damage to property and persons, service interruption, financial loss, image and reputation loss and situations that impact on students' academic performance.

The following process should be used.



D.1 STEP 1 - PROGRAM MANAGEMENT

The development of a risk management program may involve the formation of a Risk Management Steering Group, with reference to the Department's overarching policy and an implementation schedule.

D.2 STEP 2 - RISK AND BUSINESS IMPACT ANALYSIS

This step prioritises the business activities that are time critical and identifies the resources that are required to support these activities for business continuity purposes. This involves assessing the potential business impact on the Department, should key business activities be interrupted, determining the timeframes within which these business activities are to be resumed, and identifying the resources required for business continuity. The key deliverables are a list of critical business activities and their corresponding maximum acceptable outage times, and a list of business continuity resource requirements.

D.3 STEP 3 - IDENTIFY RESPONSE OPTIONS

This step involves the identification and assessment of response options to meet the Department's requirements for business continuity, covering people, IT systems and networks, premises and facilities, and data backup and offsite storage. The key deliverables are response options with supporting justifications (pros, cons, and costing) and a recommendation on the most appropriate option.

D.4 STEP 4 - DEVELOP RESPONSE PLAN

This step involves putting in place a response team structure, developing processes for incident notification and escalation, and documenting the Business Continuity Management Plans. This is also when initial implementation of the response option is carried out, such as procurement of backup equipment and commissioning of alternate facilities. The key deliverables are response teams, Business Continuity Management Plans and facilities for business continuity.

D.5 STEP 5 - TRAIN, EXERCISE AND MAINTAIN

This step ensures that what has been developed and documented will actually work to continue delivering critical business activities when a crisis arises. This involves training relevant employees on the use of the Business Continuity Management Plan, conducting exercises to validate the completeness and accuracy of the Plan, and putting in place a schedule for the on-going maintenance of the Plan. The key deliverables are schedules for training, testing and maintenance, and the actual conduct of these activities.

APPENDIX E HISTORY OF CHANGES

Effective Date	Last Update Date	Policy version no	Ref No.	Notes
18 May 2010	1 August 2012	1.2	D12/0501158	Amended an erroneous numeral 4 that appeared at the head of the third column of the Risk Rating table at Appendix C.4 as per D12/0470346.
18 May 2010	25 June 2015	1.3	D15/0248588	Updated contact details D15/0198137
18 May 2010	29 September 2015	1.4	D15/0394289	Updated references to *Public Sector Commissioner's Circular* and *Treasurer's Instruction TI 825.* D15/0394179
18 May 2010	31 August 2018	1.5	D18/0388738	Minor updates to contact information to reflect organisational changes D18/0388673.
18 May 2010	18 March 2021	1.6	D21/0145765	Minor changes to update content D21/0145764