



New South Wales
Government

Hon Carmel Tebbutt MLC
Minister for Education and Training

Mr M Brown MP
Chairman
Public Accounts Committee
Parliament House
Macquarie Street
SYDNEY NSW 2000

RML 05/1581
DGL 05/519

Dear Mr ^{Nat}Brown

I refer to your letter dated 23 March 2005 regarding the inquiry into Risk Management in the NSW Public Sector. I note you also wrote to the Director-General of the Department of Education and Training on this matter.


I have included the submission **TAB A** from the Department of Education and training outlining its response to managing its business risks.

The Department of Education and Training has completed the survey questionnaire **TAB B**.

The following are the names of appropriate officers within the Department of Education and Training who can act as the first point of contact for the Committee:

Bill Middleton	Director of Audit	Telephone 02 9561 8913
Terence Purser	Manager (Management Audit)	Telephone 02 9244 5756

Yours sincerely


Hon Carmel Tebbutt MLC
Minister for Education and Training

17 MAY 2005

DEPARTMENT OF EDUCATION AND TRAINING

Submission for the Public Accounts Committee

SUBMISSION TO PUBLIC ACCOUNTS COMMITTEE'S INQUIRY INTO RISK MANAGEMENT – QUESTIONNAIRE FOR SELECTED AGENCIES

I refer to your letter received on 29 March 2005, regarding the inquiry into Risk Management in the NSW Public Sector.

My comments on each of the terms of reference are as follows:

How the NSW public sector has responded to the recommendations in the 2002 Auditor-General's Report to Parliament – managing Risk in the NSW Public Sector

The Auditor-General's Report on Managing Risk has been a useful catalyst to emphasise the need for appropriate risk management systems within NSW agencies. It must be remembered that in the wider context of corporate governance, a robust risk management framework is but one element. There is a general need to improve corporate governance of public sector agencies.

How NSW public sector agencies are implementing the requirements of the new Standard.

The Auditor-General's report and the new Risk Management Standard provide comprehensive guidance on the identification of individual risks and their management. However, in terms of development of a comprehensive risk management framework, there is only limited guidance on a standard risk framework model for public sector agencies.

In response to the Auditor-General's report, a steering committee to implement a risk management framework for the Department of Education and Training (DET) was first established in November 2002.

The Department's restructure in 2003 delayed the process due to the need to ensure risk management activities were integrated into the new structure.

In March 2004, the Director-General instigated a departmental wide corporate governance review to provide a wider perspective of what improvements could be made to the whole departmental governance framework. This review identified that some major improvements were required in Strategic Planning, Risk Management and Project Management. Action is in progress to remedy these findings.

A Results and Services Plan (RSP) is being developed for the department in consultation with Treasury. The RSP will form the basis of business plans and reporting processes. It is intended to integrate into the RSP a risk management

process to ensure strategic and operational risks are regularly identified, documented, managed and reported.

A draft DET risk management policy (**Appendix 1**) and draft detailed risk management guidelines (**Appendix 2**), reflecting the new standard, were circulated to senior management for comment in December 2004 and are currently being amended for implementation in 2005. The risk management policy makes risk management a responsibility of all staff and risk management responsibilities have been included in all senior executive service performance agreements.

In addition, DET has established specialist areas that provide guidance and support for specific risk areas such as the OH&S Directorate and the Safety and Security Directorate. DET has also established specific policies and procedures to assist in the management of various specific critical risks including: management of serious incidents at schools and colleges; child protection policy and procedures; business continuity planning; and more recently an environmental policy.

The level of progress towards development of better risk management practice in the NSW public sector.

Better risk management practices in their own right are not seen as invariably leading to better managed organizations but progress towards adequately embedding better risk management practices into the management and culture of an agency would be a more critical indicator.

Once the DET policy is fully implemented, the department would be in a position to meet all the key recommendations made in the Auditor-General's report and the requirements outlined in the new risk management standard.



Bill Middleton
DIRECTOR, AUDIT

22/4/05

ENTERPRISE RISK MANAGEMENT – DET POLICY

1. Policy Statement	<p>1.1 The Department of Education and Training (DET) functions within an Enterprise Risk Management (ERM) framework to minimise adverse effects and enhance potential opportunities to help achieve organisational objectives.</p> <p>1.2 This policy sets a common approach and responsibilities for all staff to systematically manage risk and maximise opportunities consistent with the Australian Standard on Risk Management.</p> <p>1.3 Risk Management is performed at three levels within DET:</p> <p style="padding-left: 20px;">1.3.1 Strategic – this relates to risks associated with DET carrying out its business objectives as articulated in the Priorities Statement. These risks are identified, documented and managed in the organisation’s business plans down to the business unit level (Regions and Directorates). Existing reporting systems are used to report achievement of objectives and management of identified risks.</p> <p style="padding-left: 20px;">1.3.2 Operational – this relates to the management of risks associated with the DET business units (Regions and Directorates) meeting their specific objectives. These risks are identified, documented and managed in the unit’s operational plans. Existing reporting systems are used to report achievement of objectives and management of identified risks.</p> <p style="padding-left: 20px;">1.3.3 Specialist Areas – To support both Strategic and Operational risk management, DET has established several specialist areas that provide guidance and support in specific areas eg Safety & Security Directorate and OH&S Directorate. In addition, DET has established specific policies and procedures to assist units to manage various specific risks eg Managing Serious Incidents, Child Protection Policy, Corruption Prevention Policy, Business Continuity Planning and Environmental Management.</p>
2. Contact	Director Audit, (02) 9561 8234
3. Unique Identifier	PD/2004/0036/V001

4. Applicability

This policy applies to all DET staff and management processes including strategic planning, business planning, policy development, project management and decision making at both the strategic and operational levels.

5. Context

5.1 The NSW Treasury

- 5.1.1 in 1997 developed the *Risk Management and Internal Control Toolkit* to assist public sector agencies implement a risk management and internal control framework. In addition, this *Toolkit* facilitates agencies’ self-assessment of their position in relation to current best practice and
- 5.1.2 through *A Guide to Service and Resource Allocation Agreement Outcome Statements 2003-04*, provides instructions and advice to government agencies as part of the Budget process. Under Section 5 of this Guide the DET is required to identify risks, risk indicators and risk management strategies.

5.2 The Audit Office of NSW *Performance Audit Report: Managing Risk in the NSW Public Sector*, June 2002, contains the recommendation that the Government "require all agencies in the public sector to manage risks in accordance with accepted standards". In addition, the report recommends that the Government "require the attestation and risk management procedures adopted to be included in Annual Reports."

5.3 The Australian National Training Authority has developed Standards for Registered Training Organisations (RTOs). Standard 1, *Systems for quality training and assessment*, includes the implementation of procedures to "identify and manage risks concerned with compliance with the Standards for Registered Training Organisations". [Standard 1.8 i].

5.4 In March 2003, the Australian Stock Exchange issued *Corporate Governance Guidelines* which included 10 principles of best practice. The establishment of a sound system of risk oversight and management and internal control is noted as Principle 7.

5.5 This policy should be read in conjunction with other DET risk related policies in the areas of Occupational Health & Safety, Child Protection, Corruption Prevention and Business Continuity Planning and Environmental Management.

6 Responsibilities and Delegations

6.1 Board of Management

- establishment of ERM in the DET
- development of the ERM framework incorporating DET corporate plans and performance agreements
- monitoring and review of reports as part of the corporate reporting framework
- monitoring and review of ERM implementation in the DET

6.2 Senior Executive Service and Senior Officers

- ensuring that risk management is integral to organisational unit planning
- preparation and monitoring of risk management plans
- report the management of risk as part of the corporate reporting framework

6.3 All staff

All DET staff are responsible for the management of risk. This includes:

- familiarisation with the risk management process and its application within their areas of responsibility
- participation in the identification, assessment, reporting and management of risk

7 Monitoring, Evaluation and Reporting Requirements

All Senior Executive Service and Senior Officers are responsible for monitoring and evaluating the operation of this policy within their area of responsibility and reporting the management of risk as part of the corporate reporting framework.

8 Implementation of the Policy Statement

[Click here](#) to link to an index of all relevant procedures, standards, guidelines and forms to facilitate implementation of enterprise risk management within the DET.

NEW SOUTH WALES
DEPARTMENT
OF EDUCATION
AND TRAINING



ENTERPRISE RISK MANAGEMENT IN THE DEPARTMENT OF EDUCATION & TRAINING

GUIDELINES

FOREWORD

The Department of Education and Training (DET) is committed to a structured and systematic approach to the management of risk across the whole organisation in accordance with current industry standards and best practice.

Risk management is an integral part of good business practice and involves the implementation of cost effective strategies such as foreseeing potentially damaging events; implementing minimisation actions, and providing decision makers with information to assess acceptable risks.

Enterprise Risk Management encapsulates the extension of Risk Management from a purely business unit focus to an organisational wide operational and strategic focus. This is designed to identify the whole range and relative priority of risks that have to be managed by the organisation as a whole and allow all reasonable steps including action if necessary at Board of Management level to ensure these risks are adequately managed.

Risks are continuously emerging due to the increasing complexity and scope of DET operations, the changing nature of our environment and our relationships with stakeholders and the increasing need for accountability.

The Department's Enterprise Risk Management policy and guidelines bring together and build on existing risk management activities through the implementation of an enterprise risk management framework.

All staff have a responsibility for managing risk. Risk Management is compulsory as part of the *Enterprise Risk Management – DET Policy*. These guidelines are provided to assist in the implementation of this Policy and should be used as a guide only. However, you must document the risk methodology you choose to use to manage risk. These guidelines will be located on the DET intranet and should be read in conjunction with the *Enterprise Risk Management – DET Policy*.

These guidelines also provide a framework for managing risk across the DET in a manner that is holistic, integrated, inclusive and consistent. They outline the steps to follow in the development of risk management plans.

Andrew Cappie-Wood
DIRECTOR-GENERAL OF EDUCATION AND TRAINING
MANAGING DIRECTOR TAFE NSW

CONTENTS

1. The Enterprise Risk Management Framework
2. Definition of Terms
3. The Risk Management Process
 - Establish Context
 - Identify Risks
 - Analyse Risks
 - Evaluate and Rank Risks
 - Treat Risks
 - Monitor and Review
 - Communicate and Consult
4. Associated Documents and Forms
 - Form 1 – Risk Assessment Context
 - Form 2 – Risk Register
 - Form 3 – Risk Management Plan
5. References

1. THE ENTERPRISE RISK MANAGEMENT FRAMEWORK

The Enterprise Risk Management Framework ensures that risk is managed across the DET in a holistic manner, is integrated into the Department's culture, business practices and business plans, is inclusive of all levels of staff and is applied in a consistent manner.

Risk Management is performed at three levels within DET:

- Strategic – this relates to risks associated with DET carrying out its business objectives as articulated in the Strategic Priorities Statement. Risks are identified, documented and managed in the organisation's business plans down to the business unit level (Regions, Directorates). Existing corporate reporting systems are used to report achievement of objectives and management of identified risks.
- Operational – this relates to the management of risks associated with the DET business units (Regions, Directorates) meeting their objectives. Risks are identified, documented and managed in the unit's operational plans. Existing reporting systems are used to report achievement of objectives and management of identified risks.
- Specialist Areas – To support both Strategic and Operational risk management, DET has established several specialist areas that provide guidance and support in specific areas eg School Safety & Security Directorate and the OH&S Directorate. In addition, DET has established many specific policies and procedures to assist units to manage various specific risks eg Managing Serious Incidents Procedures and Child Protection Policy & Procedures.

This framework provides for consistent and ongoing processes for identifying, analysing, treating/responding to, monitoring and reporting on risk so that any changes in risk exposures or areas requiring immediate action are highlighted promptly so that appropriate improvement actions can be implemented.

The framework provides for the identification and assignment of risk ownership to those who have the authority and responsibility to ensure it is managed.

2. DEFINITION OF TERMS

Acceptable level of risk

The acceptable level of risk reflects the decision by management to accept the likelihood and consequences of a risk. This is also known as the organisation's risk appetite.

Consequence

The outcomes associated with a risk occurring eg the loss, injury, disadvantage or gain.

Control

Any measure or action that reduces the likelihood or consequence of a risk materialising.

Inherent Risk Level

The level of risk calculated (using likelihood and consequence criteria) in the absence of existing controls.

Likelihood

Likelihood is the qualitative description of the probability or frequency of a risk occurring.

Residual Risk Level

The level of risk calculated (using likelihood and consequence criteria) after considering the existing control environment.

Risk

Risk is the chance of something happening that will have an impact on achieving the organisation's objectives. It is measured in terms of the likelihood of occurrence and the magnitude of the consequences.

Risk Management Plan

The risk assessment output document prepared by each business unit which contains those risks not at an acceptable level and the treatments to better mitigate those risks.

Stakeholders

Stakeholders are those people and organisations who may affect, be affected by, or perceive themselves to be affected by, a decision or activity of DET.

3. THE RISK MANAGEMENT PROCESS

Risk Management involves the identification and treatment of risks that impact on the organisational strategies used to achieve corporate goals. Therefore it is important to understand the organisation – its capabilities, goals, objectives and the strategies in place to achieve them in order to manage those risks.

The risk management process that should be followed is described in this section and is based on the Australian Standard on Risk Management AS/NZS 4360:2004. This Standard provides the elements of the risk management process that will assist in the management of those risks that impact on achieving the corporate objectives. These elements are shown in the diagram below.

Risk Management Standard AS/NZS 4360:2004

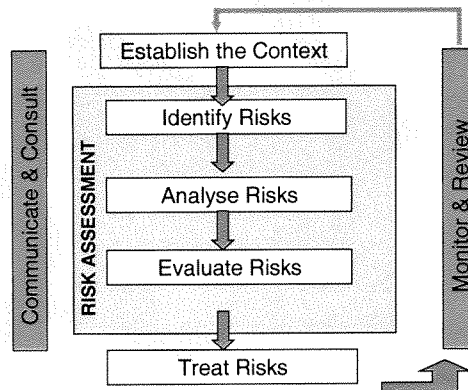


Figure 2.1: Risk Management Process- Overview

AS/NZ 4360:2004 Australian New Zealand Standard Risk Management
Standards Australia Standards New Zealand

THE OUTPUTS

You should document the risk assessment process undertaken. The forms attached are included to assist you in this and are provided as a guide only.

The outputs of the risk management process conducted at the different levels include:

Strategic Level:

- DET Business Plans

Risk Management at the strategic level is incorporated and an integral part of business planning.

The Business Plan contains the strategic risks associated with not meeting the corporate strategies and objectives. The DET Business Plans are developed by each DET Portfolio.

The Business Plans can be used by DET business units when conducting their own risk assessment. The Business Plan helps to identify the context of the risk assessment and ensures that risks identified at the business unit level are relevant and aligned to the strategic level risks.

Business Unit Level:

- Business Unit Risk Register

Refer to Form 2 – Risk Register contained in Section 4 Associated Documents and Forms.

This document contains the business unit's risks and their assessment. This is developed by the business unit and is used to prepare the Business Unit Risk Management Plan.

- Business Unit Risk Management Plan

Refer to Form 3 – Risk Management Plan contained in Section 4 Associated Documents and Forms.

This document contains the implementation details of the treatments for the key risks assessed at an unacceptable level.

To assist you to prepare these documents, follow the steps below using the forms provided.

A risk assessment should be updated at least annually and or at times when new and emerging risks may arise for example, the introduction of new business products, processes, systems and or services. Each business unit should use the above risk management process, to identify, assess and manage the risks to which the DET may be exposed. The risk assessment should be conducted as part of the existing planning processes.

The risk assessment will provide business unit managers with information to assist them to make informed decisions about what major risks (remaining at an unacceptable risk level) will be reported to the Board of Management through existing corporate reporting structures.

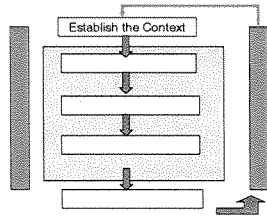
Special Areas

Where a specialist area has been established to assist business units to manage specific risks, business unit management should refer to the specific policy and guidelines related to those areas.

- Occupational Health and Safety Directorate
- Safety and Security Directorate
- Child Protection Policy
- Managing Serious Incidents Policy
- Business Continuity Policy
- Environmental Strategy
- Other

THE PROCESS

Risk Management Standard AS/NZS 4360:2004



4.1 Step 1 - Establish the Context

The purpose of this step is to define the context and scope for the risk assessment. This involves understanding the internal and external environment in which risks occur including strategic, operational, financial, competitive, stakeholder, social, cultural and legal aspects of your functions. This will provide the structure for the risk assessment tasks that follow.

To establish the context and scope for the risk assessment, you will need to identify the following five key elements.

Use Form 1 Risk Assessment Context contained in Section 4 Associated Documents and Forms to record your information.

1. *The business unit or activity to be risk assessed*

The risk assessment must be conducted at the business unit level.

Example: *Primary Education Directorate – Literacy Program*

2. *The business objective(s) for this business unit or activity and relevant Key Performance Measures*

Define what your business unit does in terms of business objectives. You need to ensure that objectives are specific, measurable, achievable, relevant and timely. This will help you focus on the risks that are directly linked to achieving the business objectives.

Identify key performance measures to check whether you have described your business objective(s) correctly.

Example:

To improve literacy by 5% for NSW Government students in years K-6 by 2005.

Key Performance Measure: NSW Basic Skills Test results

3. *The key business processes undertaken to achieve the business objectives and the environment in which they operate*

Identify the key activities and processes for the achievement of the business objective(s). Identify the environmental factors that impact on these activities or processes including legislative, social, economic, political and technological factors.

Example:

Key Processes:

*Plan Literacy Program
Implementation of Literacy Program
Monitor and review Literacy Program*

Factors :

Community expectations, compliance with legislation and program guidelines, limitation of program funding, use of technology to deliver program.

4. *The internal and external stakeholders*

Stakeholders are those people that may be affected by any of your decisions on risk management. They can be internal or external to DET.

Example:

Internal: *DET staff*

External: *Minister, unions, service providers, parents and community, suppliers.*

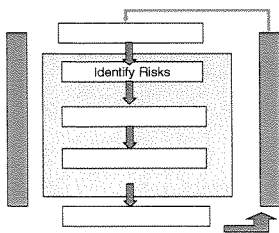
5. Management's acceptable level of risk for this activity

Risk assessments should reflect what the acceptable level of risk is for the activity as determined by Senior Executive Service or Senior Officer staff responsible for the activity.

Example:

*Acceptable Level is "Low".
All risks above this level must be managed*

Risk Management Standard AS/NZS 4360:2004



4.2 Step 2 - Identify Risks

The purpose of this step is to develop a comprehensive list of risks that impact upon the achievement of the business objective.

The context and scope of the risk assessment defined in Step 1 above will set the boundaries for which risks will be included on your list. It is critical that all risks impacting on the achievement of the business objective are identified, whether or not they are under the control of DET. If risks are not identified they will be excluded from analysis from this point onwards.

To identify risks for each of the key business processes identified in Step 1 above, ask the following questions:

What can happen? (The impact)
How and why can it happen? (The cause)

Each risk is described in terms of the impact and cause.

Example : *(Using the context information in Step 1 above)*

*“ Students’ improved literacy levels not known (impact)
because no assessment of student skills is conducted
(cause).”*

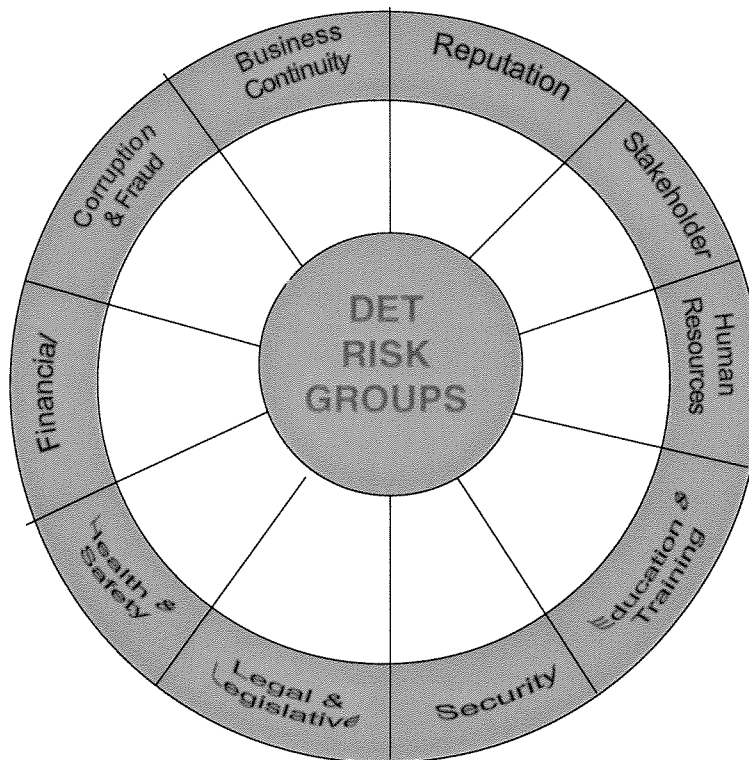
It is important that you consult with people who are knowledgeable about the activity being assessed. You can identify risks through individual staff interviews or by conducting focus group meetings and workshops. The latter is recommended where the activity is complex and involves staff in more than one area.

You can use brainstorming techniques, examination of records, observations of activities, audits and physical inspections, surveys and questionnaires to stakeholders, scenario analysis, systems analysis to help you identify risks.

Use Form 2 Risk Register contained in Section 4 Associated Documents and Forms to record your information.

DET Sources of Risk

The following ten risk categories can be used to facilitate easy identification of risks. These categories are the sources of risk i.e. where the risk can arise. Examples of risks that would be grouped in each category are also provided on the following pages. Note; the list is not exhaustive, it is provided as a guide.



The following description of each source of risk is provided to help you categorise the individual risks identified in your risk assessment:

Education & Training

This category primarily relates to risks associated with meeting the education and training objectives and strategies. Examples of drivers of risk in this category include:

- delivery, achievement, assessment and reporting of educational objectives and outcomes
- provision of quality learning environments
- provision of information and communication technologies
- school leavers with School Certificate and or Higher School Certificate
- vocational education and training
- employability of TAFE graduates
- marketing and promotion of core activities
- product development
- service delivery
- market share
- client needs
- equity
- environmental

Human Resources

This category primarily relates to risks associated with the provision and management of staff. Examples of drivers of risk in this category include:

- attracting and maintaining key staff
- staff skills and qualifications
- staff disputes

Stakeholder

This category primarily relates to risks associated with activities requiring stakeholder lobbying or strategic initiatives from the Board of Management. Examples of drivers of risk in this category include:

- changes in government
- community expectations
- legislative changes
- unions
- media
- staff associations and councils
- environmental

Reputation

This category primarily relates to risks associated with DET's reputation amongst stakeholders arising from actual or perceived poor performance in delivering services. Examples of drivers of risk in this category include:

- product and or service delivery
- stakeholder, employer and customer perceptions and expectations
- brand protection

Business Continuity

This category primarily relates to risks associated with ensuring key DET activities are able to continue in the event of major business interruptions. Examples of drivers of risk in this category include:

- technological change
- natural disasters
- strikes
- computer breakdowns

Corruption & Fraud

This category primarily relates to risks associated with corrupt and fraudulent activities. Examples of drivers of risk in this category include:

- theft
- misappropriation
- conflicts of interest
- bribery
- falsification of records
- academic fraud
- favouritism in recruitment
- misuse of resources including communication devices

Financial

This category primarily relates to risks associated financial processes and operations. Examples of drivers of risk in this category include:

- revenue
- expenditure
- assets and liabilities
- corporate credit cards

Health & Safety

This category primarily relates to risks associated with ensuring the health and safety of students and DET staff. Examples of drivers of risk in this category include:

- child protection
- student welfare
- staff welfare
- occupational health & safety
- environmental

Legal & Legislative

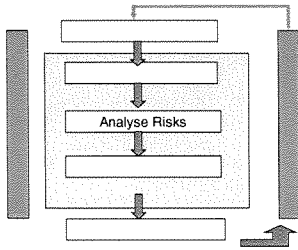
This category primarily relates to risks associated with meeting legal obligations and compliance with legislative requirements. Examples of drivers of risk in this category include:

- breaches of contract
- public liability
- professional liability
- legislative non-compliance
- industry partnerships
- environmental

Security

This category primarily relates to risks associated with provision of physical security to protect DET assets. Examples of drivers of risk in this category include:

- intellectual property
- privacy of information
- property and equipment
- data integrity



4.3 Step 3 - Analyse Risks

The purpose of this step is to calculate the level of the risks identified in Step 2 above. The risk level helps you to prioritise the risks and ensure that resources to manage risks are allocated to those of greater priority.

To calculate the level of risk, you will need to assess the likelihood of the risk occurring and the magnitude of the consequences of the risk. The product of these two values will result in the risk level.

Levels of Risk

There are two levels of risk that you can calculate.

- Inherent risk level: level of risk in the absence of any controls
- Controlled risk level: level of risk with controls in place

It is important to calculate both risk levels as this helps to determine the level of control and treatment required. First, calculate the inherent risk level. If this level is low then fewer controls and treatments are necessary. You could also eliminate some controls where the level of risk is low.

The calculation of both risk levels will assist you to direct resources to manage those risks with the highest priority.

Follow the steps below to calculate the inherent and controlled risk level for your risks.

Use Form 2 Risk Register contained in Section 4 Associated Documents and Forms to record your information.

1. Use the following criteria to help you assess the likelihood rating for each risk.

Likelihood Rating	Criteria
Almost Certain	Risk is expected to occur in most circumstances
Likely	Risk will probably occur in most circumstances
Possible	Risk might occur at some stage
Unlikely	Risk is not expected to occur during normal operations
Rare	Risk may occur only in exceptional circumstances

2. Use the following criteria to help you assess the consequences rating for each risk.

Risk Focus	Consequence Rating				
	Insignificant <i>Little or no impact</i>	Minor <i>Impact can be absorbed by existing resources</i>	Moderate <i>Impact can be absorbed with treatment</i>	Major <i>Business unit may not meet its objectives</i>	Catastrophic <i>Business unit will not meet its objectives</i>
Education & Training	Little or no effect on operations	Effect absorbed within routine operations	Some aspects of programs/strategies compromised	Programs/strategies compromised. Adverse publicity	Programs/strategies not delivered. Ministerial inquiry
Human Resources	Little or no effect on operations	Effect absorbed within routine operations	Some aspects of programs/strategies compromised	Programs/strategies compromised. Adverse publicity. Isolated industrial action	Programs/strategies not delivered. Ongoing industrial action. Ministerial inquiry
Stakeholder	Little or no effect on operations	Effect absorbed within routine operations	Matter subject to review or changes made to operations	Community dissatisfaction Ministerial Inquiry/Parliamentary scrutiny	Resignation and or removal of Minister and or DET staff
Reputation	Little or no publicity or minor adverse publicity	Local adverse publicity	State wide adverse publicity	Sustained state wide adverse publicity Community dissatisfaction	Resignation and or removal of Minister and or DET staff
Business Continuity	Little or no disruption to services	Some disruption to operations managed by altered routine	Disruption to some operations within an area Other areas may be affected	All operations of an area are compromised Other areas are affected	Total shutdown of operations
Corruption & Fraud	Little or no effect on operations	Impact can be absorbed by DET	Impact funded within area's budget	Impact requiring additional funding from within DET	Impact requires external funding

Risk Focus	Consequence Rating				
	Insignificant <i>Little or no impact</i>	Minor <i>Impact can be absorbed by existing resources</i>	Moderate <i>Impact can be absorbed with treatment</i>	Major <i>Business unit may not meet its objectives</i>	Catastrophic <i>Business unit will not meet its objectives</i>
Financial	Loss, error or omission is below 1% of the appropriate base amount	Loss, error or omission is between 1% -5% of the appropriate base amount	Loss, error or omission is between 5% - 10% of the appropriate base amount	Loss, error or omission is between 10% - 15% of the appropriate base amount	Loss, error or omission is above 15% of the appropriate base amount
Health & Safety	Little or no loss or injury	Loss or injury but no lost work time	Loss or injury and lost work time resulting in compensation	Serious loss or injury resulting in hospitalisation and or significant compensation	Loss or injury resulting in death
Legal & Legislative	Little or no effect on operations	Effect managed at local level	Significant effect on DET operations	Isolated successful litigation against DET by other parties Ministerial inquiry	Ongoing successful litigation against DET by other parties Parliamentary scrutiny
Security	Little or no loss or damage of assets/property	Localised incidents of losses and or damages with little or no effect on operations	Localised incidents of losses and or damages with significant effect on operations	Loss or damage of assets/property in many areas	DET operations severely compromised State wide due to loss of DET assets/property

3. Use the Risk Matrix below to match the likelihood and consequence values. The intersection of these two values will give you the inherent risk level.

Risk Matrix

L I K E L I H O O D	Almost Certain			Extreme Risk		
	Likely			High Risk		
	Possible		Medium Risk			
	Unlikely					
	Rare	Low Risk				
		Insignificant	Minor	Moderate	Major	Catastrophic
C O N S E Q U E N C E						

Example :

Risk: Students' improved literacy levels not known because no assessment of student skills is conducted.

Likelihood: Possible

Consequence: Major

Inherent Risk Level: Extreme

Inherent Risk Level

4. Compare this inherent risk level with management's acceptable level of risk that was defined in Step 1 above Establish the Context.

If the inherent risk level is at or below management's acceptable level of risk then no further action is required at this stage. This risk would be subject to review in the next risk assessment.

If the inherent risk level is above management's acceptable level of risk then you will need to continue with the assessment process as outlined below.

Identify Existing Controls

5. Identify the existing practices & procedures that currently exist that minimise the risk.

Types of controls include:

- Segregation of duties
- Documentation trails
- Physical security over assets
- Checks and reconciliations
- Authority for approvals
- Audit trails
- Computer controls

Example :

Risk: Students' improved literacy levels not known because no assessment of student skills is conducted.

Existing Control:

Basic Skills Test conducted for all primary school students in Years 3 and 5.

6. Re - assess the likelihood and consequence of the risk with the existing controls in place. Plot these values on the risk matrix to give you the controlled risk level.

Example :

Risk: Students' improved literacy levels not known because no assessment of student skills is conducted.

Assessment before control:

Likelihood: Possible

Consequence: Major

Inherent Risk Level: Extreme

Existing Control:

Basic Skills Test conducted for all primary school students in Years 3 and 5.

Assessment after control:

Likelihood: Unlikely

Consequence: Moderate

Controlled Risk Level: Medium

7. You can test the effectiveness of the existing controls in minimising the risks by the amount of change from the inherent risk level to the controlled risk level.

If the controlled risk level has not changed from the inherent risk level which is at an unacceptable level, the controls are rated as **poor**.

If the controlled risk level has decreased from the inherent risk level but is still at an unacceptable level, the controls are rated as **fair**.

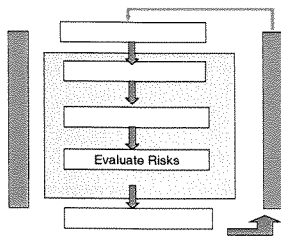
If the controlled risk level has decreased from the inherent risk level to the acceptable level then the controls are rated as **good**.

From above example:

Inherent Risk Level:	Extreme
Controlled Risk Level:	Medium
Acceptable Risk Level:	Low
<i>Control Rating:</i>	<i>Fair</i>

8. The controlled risk level determines the level of treatment required.

Extreme	(Red)	Immediate action required
High	(Orange)	Senior management attention required
Medium	(Yellow)	Management responsibility must be specified
Low	(Green)	Manage by routine procedures



4.4 Step 4 - Evaluate Risks

The purpose of this step is to develop a prioritised list of those risks that are at an unacceptable level. These risks will be included in the treatment process discussed below.

To identify the risks at an unacceptable level, compare the controlled risk level for each risk with management's acceptable level of risk that was defined in Step 1 above Establish the Context.

If the controlled risk level is at or below management's acceptable level of risk then the risk is at an acceptable level and no further risk treatment is required at this stage. This risk would be managed by ongoing monitoring and be subject to review in the next risk assessment.

If the controlled risk level is above management's acceptable level of risk then the risk is at an unacceptable level and you will need to identify the appropriate risk treatment to reduce the risk to management's acceptable level.

Use Form 3 Risk Management Plan contained in Section 4 Associated Documents and Forms to record the risks at an unacceptable level.

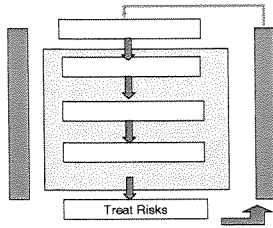
Example :

Risk: Students' improved literacy levels not known because no assessment of student skills is conducted.

Controlled Risk Level: Medium

Management's Acceptable Risk Level is: Low

Risk is at an unacceptable level – treatment required.



4.5 Step 5 - Treat Risks

The purpose of this step is to identify the most appropriate treatments for risks that are at an unacceptable level.

Use Form 3 Risk Management Plan contained in Section 4 Associated Documents and Forms to record your information.

The following are options to treat risks at an unacceptable level:

- *Avoid the risk*
Choose an alternative to achieve the same outcome.
- *Control the risk*
Develop control procedures to reduce the likelihood and or consequence of the risk.
- *Retain the risk*
Accept the risk where the treatment would not meet a cost benefit test i.e. cost of implementation of treatment are greater than the benefits received.
- *Transfer the risk*
Shift all or part of the responsibility of the risk to another party who is better able to control it. This transfer is by way of contract or by obtaining insurance.

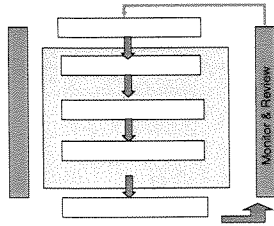
Select the best option in terms of feasibility and cost effectiveness.

Example:

Risk: Students' improved literacy levels not known because no assessment of student skills is conducted.

Controlled Risk Level: Medium

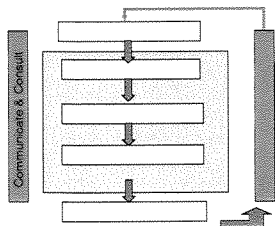
Treatment required: Assessment results are analysed and reported to management. (Control the Risk)



4.6 Step 6 - Monitor and Review

The purpose of this step is to ensure that the implementation and effectiveness of risk treatments is monitored. Risk priorities do not always stay fixed but alter with changing circumstances. The Risk Management Plan needs to be regularly maintained as new risks emerge, old ones disappear and existing risks change.

A review of the Risk Management Plan and the Risk Register should be performed at least annually. All staff can report additions, deletions and or changes to risk information at any time to the Business Unit Manager.



4.7 Step 7 - Communicate and Consult

Communication and consultation with stakeholders takes place at all steps of the risk management process. It is important that all staff responsible for managing risk and implementing risk treatments understand the reasons for the decisions.

Communication and consultation in the Department includes business units:

- reporting untreated major risks to the Board of Management through existing corporate reporting frameworks
- communicating the results of the risk assessment using the Risk Register to internal stakeholders

5. ASSOCIATED DOCUMENTS AND FORMS

- Form 1 – Risk Assessment Context
- Form 2 – Risk Register
- Form 3 – Risk Management Plan

DRAFT

RISK ASSESSMENT CONTEXT

Business unit or activity:

Business objective(s):

Key Performance Measure(s):

Key business processes:

Stakeholders:

Internal:

External:

Acceptable level of risk:

RISK MANAGEMENT PLAN

Date of Assessment:

Area / Activity:

Risk Group Ref.	Description of Risks at Unacceptable Level (Impact and Cause)	Controlled Risk Level	Acceptable Risk Level	Treatment	Responsible Officer(s) and Deadline

5. REFERENCES

AS/NZ 4360:2004 Australian New Zealand Standard Risk Management, Standards Australia Standards New Zealand, 2004.

Enterprise-Wide Risk Management Better Practice Guide for the Public Sector, Certified Practising Accountants Australia, 2002.

Risk Management Training Program, Queensland Government, February 2003.

Risk Management in the Public Sector, Risk Management Workshop conducted by Business Excellence Australia – Standards Australia 06/02 01.03.