Department of Education

Procedure

Enterprise risk management

Implementation date: 03/06/2019
Version: 7.1

Audience

Department-wide

Purpose

This procedure sets out a consistent approach for managing risk across the Department of Education (the department). This procedure is to be read in conjunction with the department's Enterprise Risk Management Framework and policy.

Overview

Risk management refers to all of the actions that we take to reduce our exposure to risk to achieve our priorities. Risk management is an ongoing, proactive process that is part of a culture of continuous improvement. Risk management is integrated into day-to-day activities and informs all aspects of our business.

Responsibilities

All staff:

- understand the department's approach to risk management as set out in the Enterprise Risk Management Framework, policy and procedure
- manage risk as part of day-to-day activities.

Staff with risk management roles:

- ensure identified risks are recorded in a risk register
- report and escalate extreme and high risks to their senior management for an appropriate response
- ensure the division or region risk register is current and up-to-date in the department's risk management system, Risk Express
- coordinate quarterly division or region risk register review and ensure deputy director-general/regional director or equivalent approval is recorded in HPRM.

Risk owners:

- manage relevant strategic, operational, project and program risks in consideration of the department's risk appetite
- regularly review the risk assessments and the current and target levels
- oversee implementation and effectiveness of risk controls and action plans.

Refer to: Enterprise Risk Management Framework; Information sheet 3 - risk assessment.

Control / action owners:

- manage implementation and effectiveness of risk controls and actions.

Senior Managers:

- ensure risks are managed according to the Enterprise Risk Management Framework, policy and procedure and recorded in a risk register and/or Risk Express
- ensure staff are aware of the department's approach to risk management
- ensure risk management is integrated into planning, review, reporting processes and project management
- escalate extreme and high risks to executive management
- prepare and implement action plans to treat risks above tolerance.

Audit and Risk Management Committee:

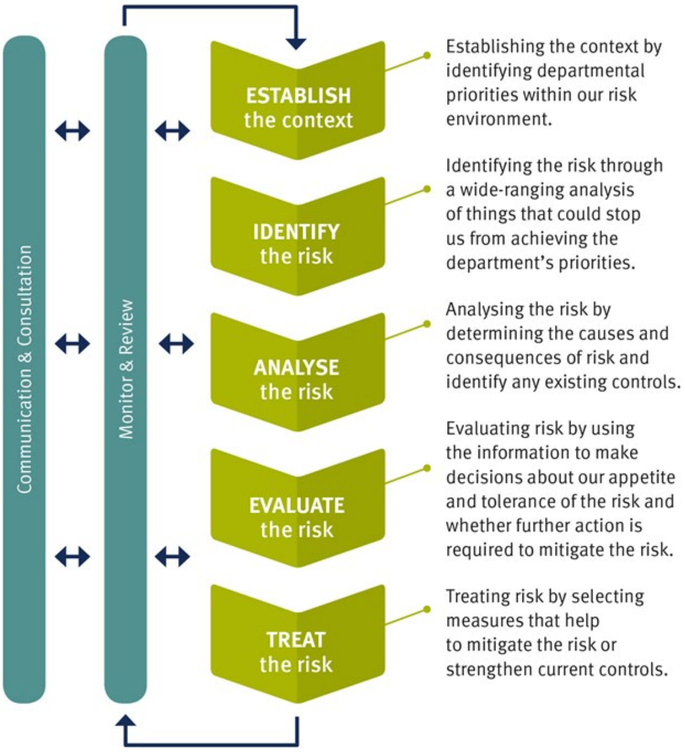
- ensure the department's risk management framework and related processes are in place and operating as intended
- consider the effectiveness of the internal control environment in managing department risks including whether controls are of an appropriate standard and functioning as intended.

Governance, Strategy and Planning:

- oversee the review of the department's risk management framework, policy, procedure and system
- provide risk management advice and guidance to business areas
- coordinate the quarterly review of the department's risk registers and report to the Executive Management Board (EMB)
- provide ongoing staff awareness training and support materials to ensure all staff are aware of the department's approach to managing risk.

Process

The department’s approach to managing risk is based on the Australian Standard (AS/NZS ISO 31000:2018):


Communication & Consultation
Monitor & Review
ESTABLISH the context
IDENTIFY the risk
ANALYSE the risk
EVALUATE the risk
TREAT the risk
Establishing the context by identifying departmental priorities within our risk environment.
Identifying the risk through a wide-ranging analysis of things that could stop us from achieving the department’s priorities.
Analysing the risk by determining the causes and consequences of risk and identify any existing controls.
Evaluating risk by using the information to make decisions about our appetite and tolerance of the risk and whether further action is required to mitigate the risk.
Treating risk by selecting measures that help to mitigate the risk or strengthen current controls.

1. Establish the context

Establish the context by identifying departmental priorities within the department’s risk environment. In establishing the context, consideration should be given to:

- defining the priorities to be achieved
- the threats that might affect the achievement of priorities
- the strengths and weaknesses of our operations
- identifying a responsible owner for managing risk
- identifying relevant stakeholders.

Refer to Enterprise Risk Management Framework; Information sheet 1 – risk category descriptions.

2. Identify the risk

To identify risks:

- generate a comprehensive list of threats and opportunities based on events that might affect the achievement of departmental priorities

- undertake a comprehensive scan of the department’s operating environment, identify the causes of risks and assess how risks affect the achievement of priorities.

There are a range of information sources and methods to help identify and assess risks, including:

- environmental, stakeholder and process analysis
- strategic and operational planning
- benchmarking against other organisations.

Refer to Information sheet 2 – identifying and describing risks.

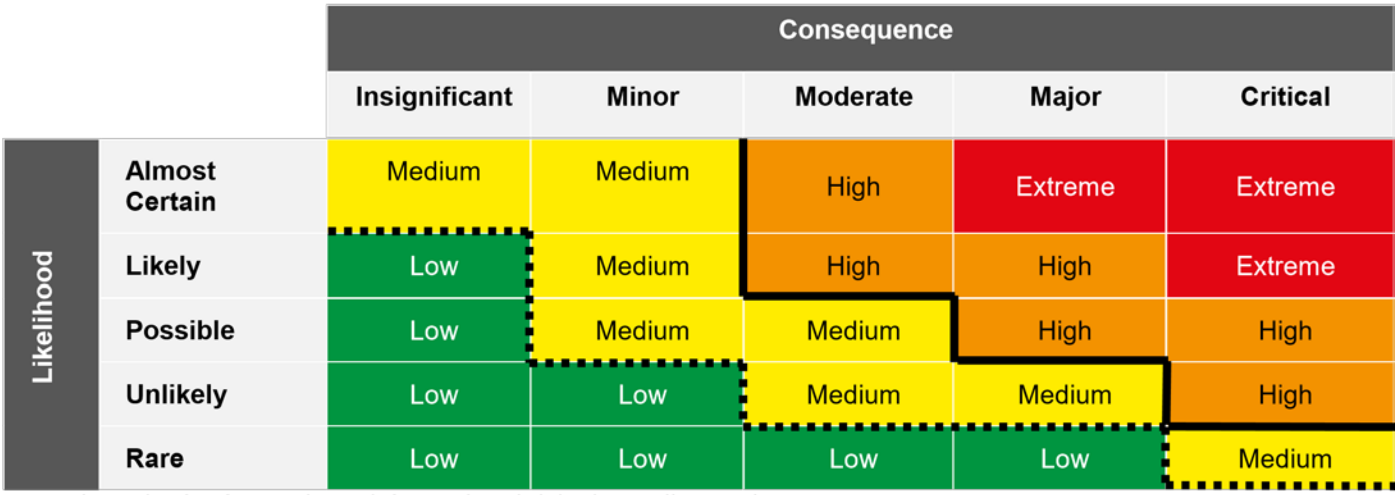
3. Analyse the risk

To analyse risks, develop an understanding of the risk and how it may impact the department. The proposed level of risk (or opportunity) is assessed according to the department’s risk appetite, and expressed in terms of the consequence and likelihood of the risk occurring:

- consequence – considers what could happen if the risk was realised
- likelihood – considers the probability of the occurrence.

3.1. Risk Matrix

The department uses a standard matrix to ensure risks are analysed and evaluated in a consistent way across the organisation.



		Consequence				
		Insignificant	Minor	Moderate	Major	Critical
Likelihood	Almost Certain	Medium	Medium	High	Extreme	Extreme
	Likely	Low	Medium	High	High	Extreme
	Possible	Low	Medium	Medium	High	High
	Unlikely	Low	Low	Medium	Medium	High
	Rare	Low	Low	Low	Low	Medium

▬ Appetite for Strategic and Operational risks is medium or low

▪▪▪▪ Appetite for Enterprise risks is low

4. Evaluate the risk

To evaluate risks, consider the identified and assessed risks to determine which risks require treatment and prioritise for attention. To determine whether a risk is tolerable the current risk level is compared with the target risk level:

- current risk level is determined by considering the department’s risk appetite and how existing controls modify the risk (or opportunity)

Queensland Government

- target risk level is determined by considering the department's risk appetite, and after applying controls/actions to reduce the impact of the risk to an acceptable level (or to maximise the opportunity).

For example, if the current level is rated high, and its risk appetite is medium, then further risk actions/treatments are required. Treatments can then be prioritised for action.

Refer to: Information sheet 3 – risk assessment; Information sheet 4 – risk consequence categories.

5. Treat the risk

Once the risk context has been established and the risks have been assessed, efficient and effective risk treatments must be determined. Most documented risk treatments reflect the controls and actions embedded in the department's policies, procedures and practices.

- a control is any permanent, on-going measure that modifies risk
- an action is a temporary process or measure applied to achieve the target level of risk.

For more information on the types of controls and actions that may be implemented to treat a risk refer to Information sheet 5 – controls and actions; Information sheet 6 – control improvement.

Definitions

Action	A new strategy to further reduce the likelihood or consequence of a risk after controls are applied.
Action owner	Position responsible for implementing actions.
Consequence	Impact of an event.
Control	Pre-existing strategies, processes or practices used to reduce the likelihood or consequence of a risk.
Control owner	Position responsible for implementing and monitoring the ongoing effectiveness of a control.
Current risk level	Level of risk with controls in place and before actions are applied.
Delivery risk	Risks associated with the delivery of services.
Enterprise risk	Areas of lowest appetite that can have a significant impact on the department achieving its priorities. To be assessed by all business areas.
Enterprise Risk Management Framework	Components that provide the departmental arrangements for designing, implementing, monitoring, reviewing and continually improving risk management.
Event	An occurrence or a change.

External risk	Risks beyond the direct control of the department.
Likelihood	Chance or probability of the risk occurring as a result of an event.
Local risk	A risk that may affect the day-to-day operations of a work area.
Mitigate	The effect of controls and actions to reduce the likelihood or consequence of a risk.
Operational risk	Risks that may affect the achievement of objectives.
Program risk	Threats emerging from the coordination of projects and activities e.g lack of consensus, lack of clarity on expected benefits, complications from working with diverse stakeholders, interdependencies, lack of funding and poor planning resulting in unrealistic timeframes
Project risk	Threats emerging from activities directed to delivering a unique product or service e.g lack of clarity of customer requirements, lack of desired skills in project team, poor quality, scope, cost and time creep.
Risk	Effect of uncertainty on the achievement of priorities. The chance of something going wrong.
Risk appetite	Level of risk or opportunity the department is willing to accept in achieving priorities.
Risk assessment	A structured process to assess risk in AS/NZS ISO 31000:2018: Risk management – Principles and guidelines.
Risk escalation	Communicating risks requiring attention to the appropriate level of management for action.
Risk level	Expression of the effect of a risk, in terms of its likelihood and the consequence if it were to occur. Risk levels are assessed at current and target.
Risk management	Coordinated activities to direct and control an organisation with regard to risk.
Risk matrix	A tool used by the department to evaluate the current and target level of a risk.
Risk owner	Position with accountability and authority to manage a risk.
Risk register	A tool or centralised repository used to record risk, controls and actions e.g. Risk Express.
Risk source	The cause(s) of a risk.
Risk tolerance	Readiness to bear a risk to achieve priorities.
Strategic risk	A delivery, external or enterprise risk that may affect the achievement of priorities.
Tactical risk	An operational, project or program risk that may affect the achievement of priorities.
Target risk level	The risk level determined appropriate according to the department's risk appetite and after application of controls/actions.

Legislation

- *Financial Accountability Act 2009* (Qld) Part 4, Section 61 (b)
- *Work Health and Safety Act 2011* (Qld) Part 2, Division 1, Section 17
- Financial and Performance Management Standard 2009 (Qld) Division 4, Section 28

Delegations/Authorisations

- Nil

Related policies

- Enterprise Risk Management Policy
- Enterprise Risk Management Framework
- Evidence Framework
- Corporate Governance Framework
- Health, Safety and Wellbeing Management Framework
- Business Continuity Management Framework

Related procedures

- Nil

Guidelines

- Queensland Treasury – A guide to risk management
- Australian/New Zealand Standard ISO 31000:2018 Risk Management – Principles and Guidelines

Supporting information/websites

- Strategic Plan
- Enterprise Portfolio and Planning (DoE employees only)
- Curriculum Activity Risk Assessment (CARA)
- Information sheet 1 – risk category descriptions
- Information sheet 2 – identifying and describing risks
- Information sheet 3 – risk assessment
- Information sheet 4 – risk consequence categories
- Information sheet 5 – controls and actions
- Information sheet 6 – control improvement

Contact

For more information, please contact:

Governance, Strategy and Planning

Phone: (07) 3513 6914

Email: enterprise.riskmanagement@qed.qld.gov.au

Review date

01/11/2019

Superseded versions

Previous seven years shown. Minor version updates not included.

2.0	FNM-PR-003: Risk Management
3.0	FNM-PR-003: Risk Management
4.0	Risk Management
5.0	Enterprise Risk Management
6.0	Enterprise Risk Management
7.0	Enterprise Risk Management

Creative Commons Licence