Procedure

Enterprise risk management procedure

Version: 7.4 | **Version effective**: 06/08/2021

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 we take to reduce our exposure to risk to achieve our objectives. It facilitates continuous improvement by linking risks to organisational planning and performance reporting. 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 local risks are recorded in a risk register
- report and escalate risks that are above the department's risk appetite to senior management for an appropriate response
- ensure the division or regional risks are current and up-to-date in the department's risk register
- coordinate quarterly division or region risk register review and ensure deputy director-general/regional director approval is recorded in Content Manager.

Risk owners:

- manage relevant risks in consideration of the department's risk appetite

- regularly review the risks in the department's risk register
- oversee implementation and effectiveness of risk controls and actions.

Refer to: Enterprise Risk Management Framework; Information sheet 2 - Assessing risk.

Control / action owners:

- manage implementation and effectiveness of risk controls and actions.

Refer to: Enterprise Risk Management Framework; Information sheet 3 – Responding to risk – controls and actions.

Senior managers:

- ensure risks are managed according to the Enterprise Risk Management Framework, policy and procedure and recorded in the department's risk register
- 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 risks assessed at extreme and high to executive management.
- prepare and implement action plans to manage 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, and procedure
- provide risk management advice and guidance to business areas
- coordinate the quarterly review of the department's risk register and report to the Executive Management Board (EMB)
- provide ongoing staff awareness, training and support materials to build capability and ensure all staff are aware of the department's approach to managing risk.

Process

The key elements of the department's process to managing risk is based on the Australian Standard (AS/NZS ISO 31000:2018):

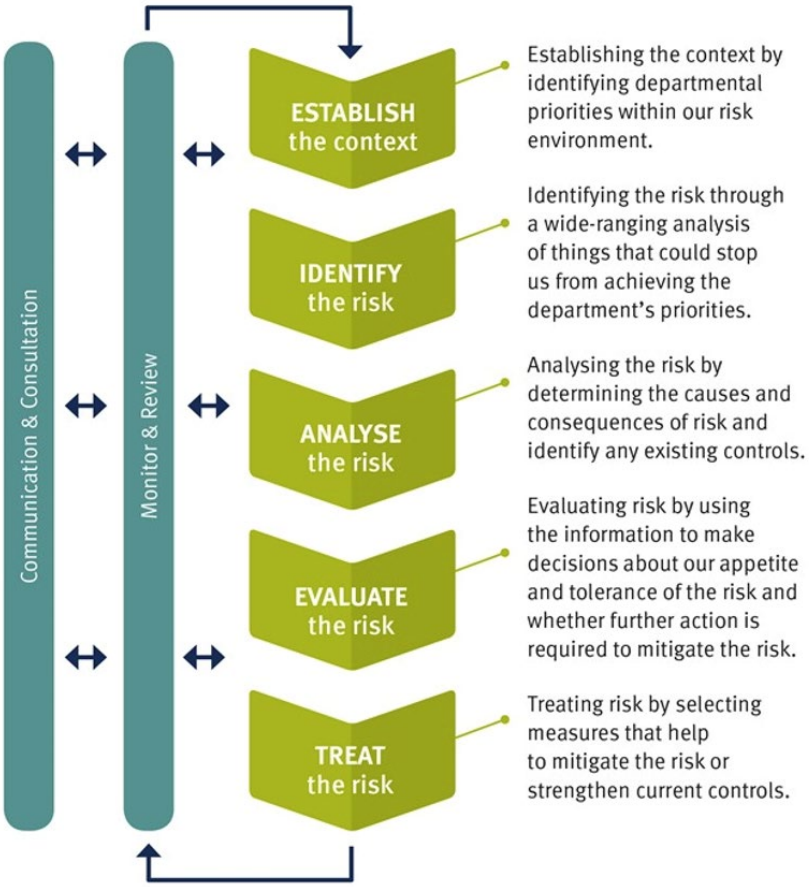

Image 1: Enterprise risk management flowchart

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 the risk category and the responsible owner
- identifying relevant stakeholders.

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

2. Identify the risk

Risk identification involves a wide-range analysis of things that could stop the department from achieving its priorities.

To identify risks:

- generate a comprehensive list of threats and opportunities based on events that might affect the achievement of departmental objectives
- undertake a comprehensive scan of the department's operating environment, identify the causes of risks and assess how risks affect the achievement of objectives.

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.

The department is willing to accept a higher level of risk when pursuing innovation and opportunities that further its strategic objectives to give all children a great start, engage young people in learning and creating safe, fair and productive workplaces and communities. When considering a new or innovative idea, use Information sheet 5 – Ideas, innovation and risk to guide you.

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.

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

- **current risk level** is determined by considering how existing controls modify the risk (or opportunity) before actions are applied
- **target risk level** is determined by considering the department's risk appetite, and after applying further controls/actions to reduce the impact of the risk to an acceptable level (or to maximise the opportunity).

The risk matrix is provided in Information sheet 2 –Assessing risk.

4. Evaluate the risk

To determine whether a risk is within the department's risk appetite, the current level is compared with the target level. This informs whether further action is required to mitigate the risks.

For example, if the current risk level is rated high, and its risk appetite is medium, then further controls and actions are required.

Refer to: Risk appetite statement and categories; Information sheet 2 –Assessing risk; Principal's risk control checklist (DoE employees only); Information sheet 4 – Risk consequence categories.

5. Respond to the risk (treat the risk)

Once the risk context has been established and the risks have been assessed, efficient and effective controls and actions must be determined. Controls and actions should help mitigate the risk or strengthen current controls.

- **controls** are an existing strategy used to maintain or modify a risk and may include any process, policy or practice and are an ongoing function of the business
- **actions** are a new planned, temporary strategy applied to maintain or achieve the target level of risk after controls are applied. Actions are undertaken in a pre-determined time-frame
- an **action can transition to a control** if the strategy becomes an ongoing function of the business.

A Principal's risk control checklist (DoE employees only) is a tool designed to assist principals to manage risk and meet their legislative obligations in the department's areas of lowest risk appetite. The actions in this checklist are a summary of key controls related to the four enterprise risks and align to departmental policies and procedures. They are not additional requirements.

For more information on the types of controls and actions that may be implemented to respond to a risk refer to Information sheet 3 – Responding to risk – controls and actions;

After determining efficient and effective controls and actions, risks should be reported using the department's risk register. The ongoing review of risks and executive oversight and scrutiny ensures appropriate governance.

Definitions

Term	Definition
Action	A new planned, temporary strategy applied to maintain or achieve the target level of risk after controls are applied. Actions are undertaken in a pre-determined time-frame
Action owner	Position responsible for implementing actions
Consequence	The outcome of an event which affects the department's ability to achieve its objectives
Control	An existing strategy used to maintain or modify a risk and may include any process, policy or practice and are an ongoing function of the business
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

Term	Definition
Enterprise risk	Areas of lowest appetite that can have a significant impact on the department achieving its objectives. 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 of a particular set of circumstances. An event can be something that is expected which does not happen, or something that is not expected which does happen
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
Modify	The effect of controls and actions to change 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 objectives
Risk appetite	Level of risk or opportunity the department is willing to accept in achieving objectives
Risk assessment	A structured process of risk identification and analysis
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

Term	Definition
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	A cause that has potential to give rise to a risk
Risk tolerance	The variation from the pre-determined risk appetite the department is prepared to accept
Strategic risk	A delivery, external or enterprise risk that may affect the achievement of objectives
Tactical risk	An operational, project or program risk that may affect the achievement of objectives
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 2019 (Qld) Division 4, Section 23

Delegations/Authorisations

- Nil

Policies and procedures in this group

- Enterprise risk management policy

Supporting information for this procedure

- Information sheet 1 – Risk category descriptions
- Information sheet 2 – Assessing risk
- Information sheet 3 – Responding to risk – controls and actions
- Information sheet 4 – Risk consequence categories
- Information sheet 5 – Ideas, innovation and risk
- Risk appetite statement and categories

Other resources

- Enterprise Risk Management Framework
- Evidence Framework
- Corporate Governance Framework
- Health, Safety and Wellbeing Management Framework
- Business Continuity Management Framework
- A Guide to Risk Management, The State of Queensland (Queensland Treasury) July 2011
- Australian/New Zealand Standard ISO 31000:2018 Risk Management – Guidelines
- Strategic Plan
- Enterprise Portfolio and Planning (DoE employees only)
- Curriculum Activity Risk Assessment (CARA)
- Principal's risk control checklist (DoE employees only)

Contact

For more information, please contact:

Governance, Strategy and Planning
Phone: (07) 3513 6914
Email: enterprise.riskmanagement@qed.qld.gov.au

Review date

1/11/2019

Superseded versions

Previous seven years shown. Minor version updates not included.

6.0 Enterprise Risk Management

7.0 Enterprise risk management

Creative Commons licence