Policy

Enterprise risk management policy

Version: 2.2 | **Version effective**: 04/02/2020

Audience

Department-wide

Purpose

This policy supports the Department of Education's (the department's) approach to risk management as set out in the Enterprise Risk Management Framework and is based on the Australian Standard on Risk management – Guidelines (AS/NZS ISO 31000:2018).

Policy statement

The Department of Education is committed to effective risk management to achieve better outcomes for our customers. Risks are managed according to the department's Enterprise Risk Management Framework, this policy and the Enterprise risk management procedure.

Principles

The department applies the following principles to risk management. Risk management:

- creates and protects value
- is systematic, structured and timely
- accounts for human and cultural factors
- is responsive to change
- is integrated into departmental processes and decision-making
- is transparent and inclusive
- leads to continuous improvement.

Requirements

1. The department's risk management approaach

The approach to managing risk at any level of the department involves:

- using the risk appetite to identify and assess the level of risk that can be taken
- understanding the risk environment: targeting risks that emerge from the department's operating environment
- assessing risk: applying a structured risk assessment process
- responding to risk: regularly assessing risks, identifying trends and patterns in risk and opportunities for continuous improvement
- reporting risk: providing assurance that risk is managed and escalated
- governing risk: governing risk through executive oversight in divisions, regions and schools.

2. Risk appetite

To deliver on the department's objectives, the Executive Management Board (EMB) has identified the level of risk it is prepared to accept and which is to be addressed by all business areas. These enterprise risks are the areas the department has the lowest appetite for:

- safety of children and students
- workplace health and safety of its staff and the community
- security of confidential and personal information held by the department
- fraud and corruption.

As its foundation, the department has a core requirement to comply with its legislative obligations in its pursuit of quality outcomes for children, students and the community.

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.

3. Understanding the risk environment

The risks targeted through the planning and reporting processes emerge from within our operating environment:

- **Delivery risks** are those with significant impacts to delivery outcomes
- **Enterprise risks** are risks for which the department has the lowest appetite
- **External risks** are risks beyond the direct control of the department
- **Operational risks** are risks that may affect the achievement of objectives
- **Program and project risks** are risks that may affect the achievement of programs or projects.

For more information on the department's risk environment see the Enterprise Risk Management Framework.

4. Assessing risk

The department's risk assessment process involves establishing the context, identifying and analysing the risk. Communication and consultation with internal and external stakeholders should take place throughout the process. Monitoring and reviewing risks should be incorporated into business as usual activities and be reported formally every quarter.

For more information on managing risk, see the Enterprise risk management procedure.

5. Responding to risk

Risks may be responded to in a number of ways including: monitoring and reviewing; escalating to senior management for further consideration; and reviewing risk registers to monitor existing controls and propose new controls and actions.

- Monitoring and reviewing risks regularly ensures that the risk is still relevant and that controls continue to be effective. Monitoring can include:
  - undertaking regular reviews of the risk register to ensure risks are current and that risk descriptions accurately define the threat, causes and potential consequences
  - reviewing the effectiveness of existing controls applied to risks to ensure they are operating as intended and adding actions to further support maintaining or modifying the level of the risk.
- Risks that are assessed as above the department's risk appetite are escalated for consideration by senior management/board who will decide to accept or reassess the risk and/or direct further review of controls and actions. For extreme and high risks:
  - schools escalate to regional level
  - regional offices escalate to EMB through the risk report
  - central office business areas escalate to divisional management and EMB
  - project teams escalate to project owners.

  Strategy and Performance is responsible for coordinating quarterly reporting to EMB.
- Risk registers are reviewed on a regular basis to monitor existing controls, propose further/future strategies to maintain or reduce the risk levels and set timeframes for implementation.

6. Reporting risk

Reporting risk provides assurance that risk is managed, escalated, and maintained or modify through effective controls and actions. Specifically:

- regional strategic and operational risks assessed above medium are escalated to the regional director for consideration
- divisional operational risks assessed above medium are escalated to senior management for consideration
- enterprise risks assessed above low are escalated to the regional director in regions and senior management in central office
- all risks above the department's risk appetite are escalated to EMB through quarterly reporting processes.

7. Governing risk

Risk is subject to executive oversight and scrutiny in schools, regional offices and divisions. Specifically:

- EMB receives regular risk reports
- Strategy and Performance reviews risk registers to identify trends and linkages across the department
- enterprise and delivery risks are managed by risk owners in divisions

- operational risks are managed by schools and regional offices
- program and project risks are managed by program and project owners.

Information about responsibilities can be found in the Enterprise risk management procedure.

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 within a pre-determined time-frame
Consequence	The outcome of an event which affects the department's ability to achieve its objectives
Control	An existing strategy used to maintain or reduce a risk and may include any process, policy or practice and are an ongoing function of the business
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 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
Likelihood	Chance or probability of the risk occurring as a result of an event
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	Risks 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	Risks 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

Term	Definition
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 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 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 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 procedure

Supporting information for this policy

- Enterprise Risk Management Framework

Other resources

- Corporate Governance Framework
- Health, Safety and Wellbeing Management Framework
- Business Continuity Management Framework
- Evidence 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)
- Risk appetite statement and categories

Contact

For further information, please contact:

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

Review date

1/11/2021

Superseded versions

Previous seven years shown. Minor version updates not included.

1.0 Enterprise Risk Management

2.0 Enterprise risk management

Creative Commons licence