DEPARTMENT OF EDUCATION, TRAINING AND EMPLOYMENT

Enterprise Risk Management Framework 2012–2016

Strengthening our commitment to risk management

Contents

Director-General's message

The Department of Education, Training and Employment's vision for risk management is for all decision makers to be fully informed of risks, and that risks are effectively managed in the achievement of our departmental objectives. Risk management benefits the department and our clients by enabling new ideas to be explored and potential risks to be managed to minimise their impact.

We are committed to continuing to improve our operational efficiency and find innovative ways of delivering our services to Queensland without compromising quality or lifting risks beyond a level that we are willing to accept.

Risk management plays a critical role in helping us understand the impacts and manage the risks associated with these priorities. It helps us determine an appropriate control environment and balance of strategies to address the risk so that we are using our resources efficiently and effectively. It involves making decisions and establishing governance systems that embed and support effective risk process, as well as building an organisational culture that supports alertness, openness and responsiveness to change.

The department's *Enterprise Risk Management Framework 2012-2016* sets out the key principles that guide how risk management is embedded at all levels — central office divisions, regions, schools and TAFE institutes. It outlines how the department will ensure that risk is managed effectively and efficiently.

We all need to be committed to continue to improve governance arrangements through strong leadership, responsible and ethical decision making, management and accountability, and performance improvement.

As government employees, we have a duty to carry out our activities according to required practice, and to do so with the objectives for our students, parents and stakeholders in mind.

I ask you to put into practice the systematic process of risk management to ensure that we continue to effectively deliver outcomes for Queensland.

Julie Grantham
Director-General
Department of Education, Training and Employment

Introduction

Purpose

The *Enterprise Risk Management Framework 2012-2016* (the Framework) provides the necessary foundations and organisational arrangements for managing risk across the department. The Framework outlines how the department ensures that it manages risks effectively and efficiently.

It illustrates how risk management is embedded in our organisational systems to ensure it is integrated at all levels and work contexts. It describes the key principles, elements and processes to guide all staff in effectively managing risk, making it part of our day-to-day decision-making and business practices.

The department applies risk management across the entire organisation — central office divisions, regions, schools and TAFE institutes, as well as specific functions, programs, projects and activities. Implementation of the Framework contributes to strengthening management practices, decision making and resource allocation, while at the same time protecting the public interest and maintaining trust and confidence.

Implementation of the Framework requires all staff to apply risk management principles to fulfil their responsibilities, to ensure cost-efficient and effective service delivery.

What is risk management?

A risk is defined as the effect of uncertainty (either positive or negative) on business objectives.[1]

Risk management is the coordination of activities that direct and control the department with regard to risks.[2] It is commonly accepted that risk management involves both the management of potentially adverse effects as well as the realisation of potential opportunities.

In performing our daily activities and responsibilities, risk management can be described as the collection of deliberate actions and activities that we carry out at all levels to identify, understand and manage risks to the achievement of our objectives.

Benefits of risk management

The benefits of embedding risk management at all levels of the department are:

- effective management of adverse events or opportunities that impact on our purpose and objectives
- ability to make informed decisions regarding management of potential negative effects of risk and take advantage of potential opportunities
- improved planning and performance management processes — enabling us to focus on core business service delivery and implement business improvements
- ability to direct resources to risks of greatest significance or impact
- greater organisational efficiencies through avoiding ‘surprises’
- creation of a positive organisational culture in which people understand their role in contributing to the achievement of objectives.

1 AS/NZS ISO 31000:2009 Risk management - Principles and guidelines, page 1.

2 AS/NZS ISO 31000:2009 Risk management - Principles and guidelines, page 2.

2 AS/NZS ISO 31000:2009 Risk management - Principles and guidelines, page 2.

Goals of the framework

The *Enterprise Risk Management Framework 2012-2016* aims to:

- integrate enterprise risk management within the department's performance management cycle
- communicate the benefits of risk management
- convey the department's policy, approach and attitude to risk management
- set the scope and application of risk management within the organisation
- establish the roles and responsibilities for managing risk
- set out a consistent approach for managing risks across the department, aligned with relevant standards and industry best practice
- detail the process for escalating and reporting risks
- convey the department's commitment to the periodic review and verification of the Framework and its continual improvement
- describe the resources available to assist those with accountability or responsibility for managing risks
- ensure the department meets its risk reporting obligations.

Principles underpinning the Framework

The *Australian Standard for Risk management - Principles and guidelines* (AS/NZ ISO 31000:2009) is based on 11 best practice principles. These principles underpin the Framework and guide how we effectively and efficiently manage risk at all levels.

1. **Creating and protecting value** – risk management contributes to the achievement of our objectives and improves performance in areas such as corporate governance, program and project management, and health and safety of staff and students.
2. **An integral part of all organisational processes** – risk management is not a stand-alone activity performed in isolation. Rather, it is an integral part of our governance and accountability arrangements, performance management, planning and reporting processes.
3. **Part of decision-making** – risk management aids decision-makers to make informed choices, prioritise activities and identify the most effective and efficient course of action.
4. **Explicitly addressing uncertainty** – risk management identifies the nature of uncertainty and how it can be addressed through a range of mechanisms, such as sourcing risk assessment information and implementing risk controls.
5. **Systematic, structured and timely** – risk management contributes to efficiency and to consistent, comparable and reliable results.
6. **Based on the best available information** – risk management should draw on diverse sources of historical data, expert judgment and stakeholder feedback to make evidence-based decisions. As decision-makers, we should be cognisant of the limitations of data, modelling and divergence among experts.
7. **Tailored** – risk management aligns with the internal and external environment within which we operate, and in the context of the department's risk profile.
8. **Human and cultural factors** – risk management recognises that the capabilities, perceptions and aims of people (internal and external) can aid or hinder the achievement of objectives.
9. **Transparent and inclusive** – risk management requires appropriate and timely involvement of stakeholders to ensure that it stays relevant and up to date. Involving stakeholders in decision making processes enables diverse views to be taken into account when determining risk criteria.
10. **Dynamic, iterative and responsive to change** – risk management responds swiftly to both internal and external events, changes in the environmental context and knowledge, results

of monitoring and reviewing activities, new risks that emerge and others that change or disappear.

11. **Continual improvement of the organisation** – risk management facilitates continuous improvement of our operations by developing and implementing strategies to improve risk management maturity.

Mandate and commitment

Risk management requires strong and sustained commitment by management of the organisation, as well as strategic and rigorous planning to achieve commitment at all levels.

Risk management - Principles and guidelines (AS/NZS ISO 31000:2009)

Our policy

Risk management is part of the department's strategy to *promote accountability through good governance and robust business practices*, which contributes to our strategic objective of *creating a capable, agile and sustainable organisation – we will manage our resources effectively to strengthen service delivery*.

The department is committed to embedding risk management principles and practices into its organisational culture, governance and accountability arrangements, planning, reporting, performance review, business transformation and improvement processes.

Through the Framework and its supporting processes, the department formally establishes and communicates its risk appetite, guiding staff in their actions and ability to accept and manage risks.

The department has a low appetite for risks relating to:

- health, safety and wellbeing of our students, staff and the community
- administration of finances and assets
- legislative compliance.

There is a potentially higher appetite where benefits created by potential innovation outweigh the risks. Benefits may include improved service delivery, and/or increased efficiency and effectiveness of the department's operations.

In accordance with the Framework, each divisional head will communicate their division's appetite for risk, as part of their risk assessment process.

To position the department as a risk-aware, responsive and resilient organisation, our risk management approach is directed through:

- compliance with relevant legislation, policies and procedures
- alignment with standards and better practice guides to soundly support decision making and continuous improvement of our risk management practices.

Effective risk management practice is modelled by:

- leadership demonstrated by the Director-General, the Executive Management Group (EMG) and its subcommittees, as well as senior executives, regional directors, school principals, TAFE institute directors and managers
- staff in all work contexts through their identification, analysis, evaluation, treatment, monitoring and review of risks that may impact on achieving our organisational purpose and objectives.

The scope of responsibility and accountability for risk management is everyone's business. The success of our risk management strategy relies on all staff enacting the risk management approach outlined in this Framework.

Authorities

The department's *Enterprise Risk Management Framework 2012-2016* is underpinned by the following legislation, standards, best practice guides and departmental frameworks, policy and procedures.

Legislation

The *Financial Accountability Act 2009* (section 61) requires the Director-General, as the accountable officer, to establish and maintain appropriate systems for internal control and risk management.

The *Financial and Performance Management Standard 2009* (section 28) prescribes that the agency's risk management system must provide for:

- mitigating the risk to the department and the State from unacceptable costs or losses associated with the operations of the department or statutory body, and
- managing the risks that may affect the ability of the department to continue to provide government services.

The department's legislative compliance procedure provides the department with a general guidance on legislative compliance responsibilities to ensure the Director-General, as the accountable officer, can be satisfied that all measures are being taken across the department to actively comply with relevant legislation and applicable standards.

Australian/New Zealand standard

While not mandated by legislation, the department's *Enterprise Risk Management Framework 2012-2016* aligns with the *Australian/New Zealand Standard ISO 31000:2009 Risk management – Principles and guidelines (AS/NZS ISO 31000).*

AS/NZ ISO 31000:2009 has identified the relationship between the principles for managing risk, the Framework in which it occurs and the risk management process using five interrelated elements.

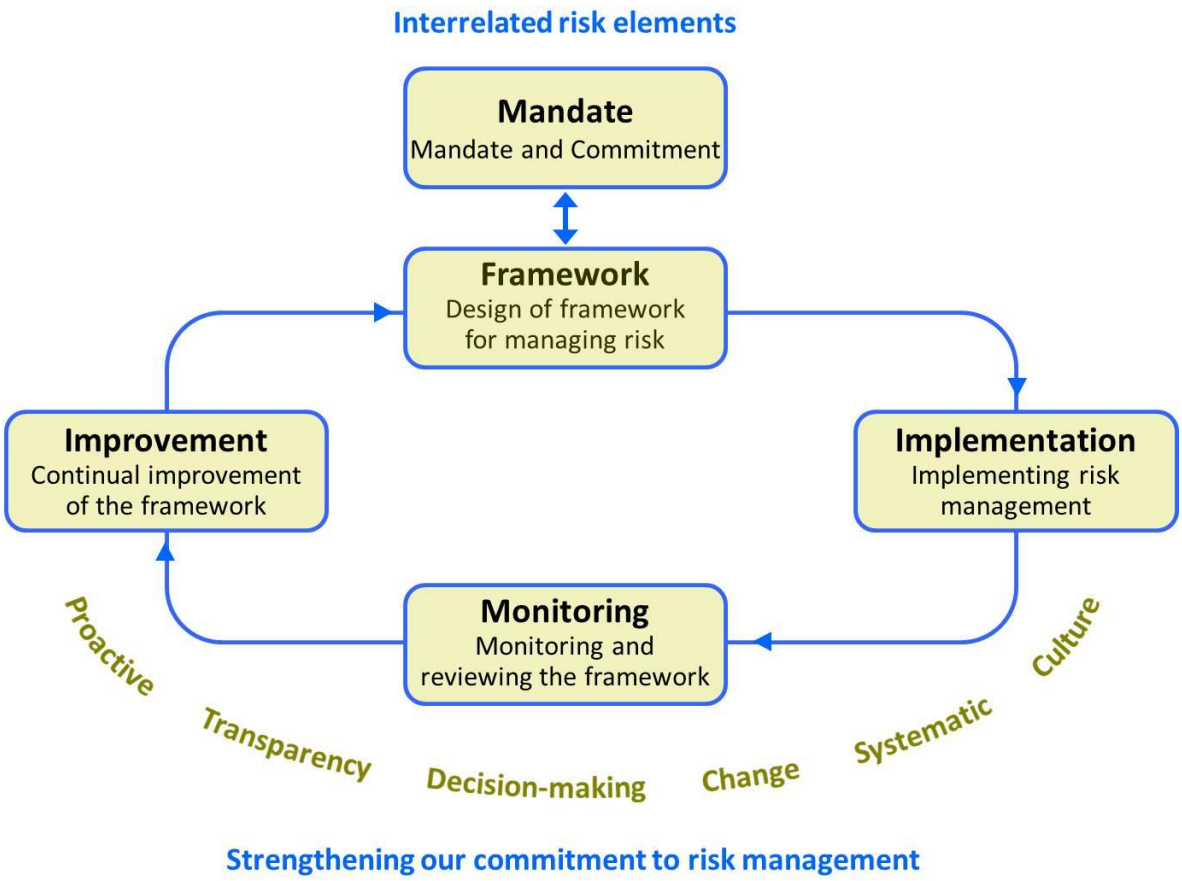


Diagram adapted from Australian Standard for Risk management - Principles and guidelines (AS/NZ ISO 31000:2009).

Whole-of-government guidelines

Queensland Treasury and the Department of the Premier and Cabinet have collaborated to develop *A Guide to Risk Management*. The guide is not mandatory, however application of the guide is intended to encourage better practice and support accountable officers in the implementation of effective risk management practices at all levels within their agency. The Framework is consistent with this guide.

Department's governance Framework

The department's governance Framework is based on principles of best practice public sector governance. Effective risk management is identified as one of the seven elements:

- **direction** — a mutual understanding of our purpose and direction, through planning and resource allocation
- **alignment** — functions, structures and culture that align with our organisational goals through leadership and sound governance
- **accountabilities** — clear and transparent accountabilities through legislative compliance, information management and corporate reporting
- **expectations** — organisation-wide understanding of performance and behavioural expectations, through effective communication and the implementation of best practice public sector management practices
- **delivery** — quality service delivery through effective program and resource management, and monitoring, reviewing and reporting processes

- **improvement** — improving organisational and individual performance through review, intervention, capacity building and internal control mechanisms
- **risk management** – managing risk within the department through adoption.

Each element contributes to, and supports the other elements in the Framework.

A framework for managing risk

> Risk management should be implemented by ensuring that the risk management process is applied at all relevant levels and functions of the organisation as part of its practices and processes.
>
> *Risk management - Principles and guidelines* (AS/NZS ISO 31000:2009)

An overview of the Framework is provided in Figure 1. The diagram illustrates the key elements necessary for managing risk, and the integration of these elements at all levels and in all work contexts. These elements are:

- risk hierarchy
- risk governance & accountabilities
- risk system.

Risk hierarchy

The department's integrated business planning system cascades from the department's strategic plan through to operational plans and program plans, through to work unit and project plans, and distilled into individual performance and development plans. The planning cycles provides an opportunity for central office division, regions and TAFE institutes to undertake analysis regarding emerging or known risks that may impact on their purpose and objectives.

While it is important to ensure that the department is 'doing risk management right', it is equally important to 'do the right risk management'. This includes having processes in place so that the appropriate levels of management have oversight of the different levels of risk across the department.

In the Framework, there are three levels of risk – strategic, corporate and operational. The risk hierarchy defines accountability for identifying, treating, monitoring, communicating and managing risks throughout the organisation.

The risk hierarchy illustrated in Figure 1 demonstrates the relationship between the cascading level of plans and the three levels of risk hierarchy, as well as a clear line of sight from the department's high level strategies to individual performance plans. Further articulation of this relationship is outlined in Table 1.

Figure 1 : *Enterprise Risk Management Framework 2012-2016*: An overview

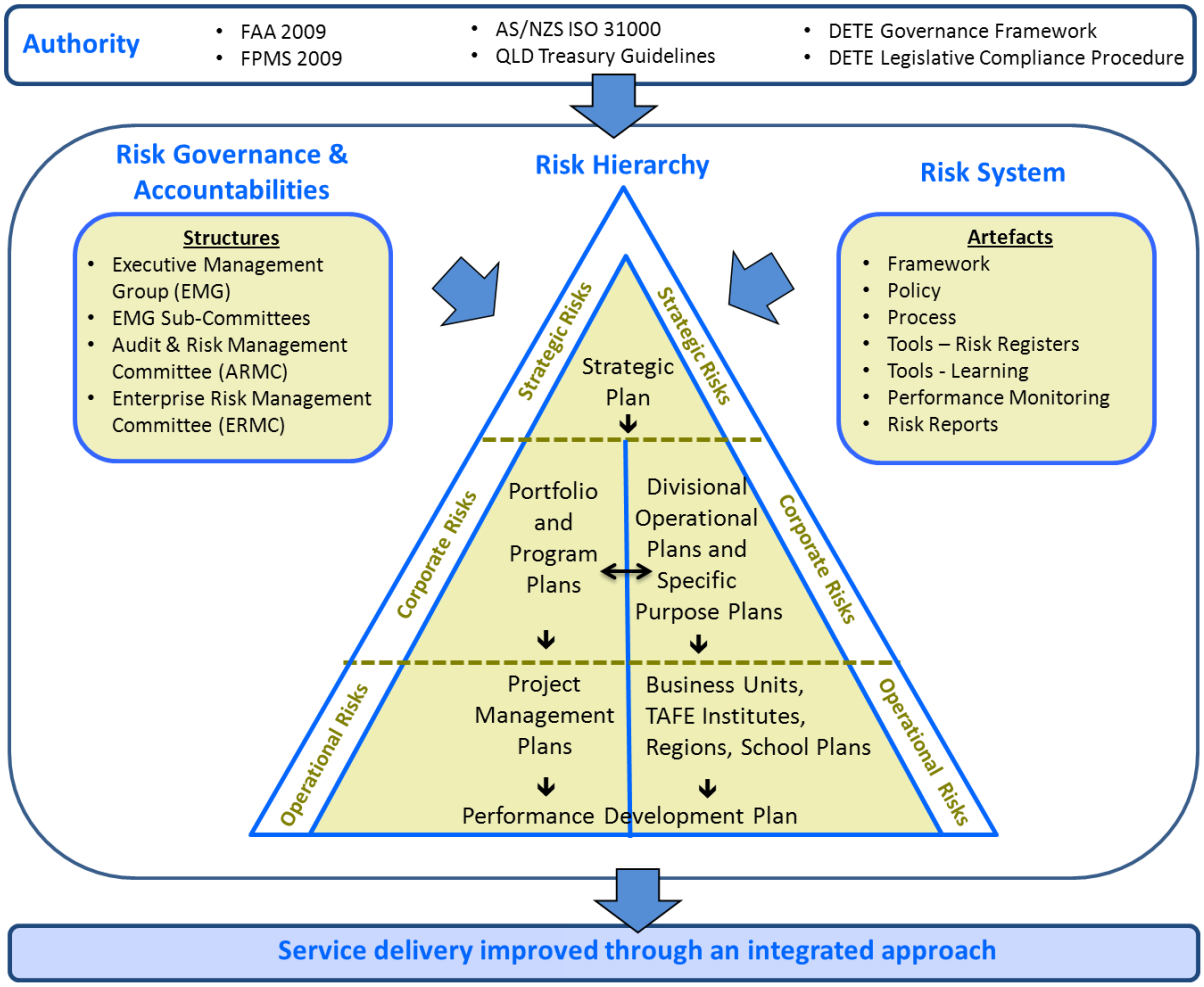


Table 1: Relationship between plans and hierarchy of risk

Plans	Hierarchy of Risk	Accountability
Strategic Plan • The Strategic Plan describes the common purpose and direction of the agency, identifies key priorities and strategies to achieve objectives and sets the policy agenda for the next four-year planning cycle.	**Strategic Risks** • Risks that may have a positive or negative effect on achieving the department's strategic purpose and objectives. • Also includes inter-departmental and whole-of-government risks, as well as high and extreme risks that may affect the achievement of objectives across more than one division. • Risks at this level affect the decisions made around whole-of-government and organisational priorities, resource allocation, and tolerance and acceptance of risk.	**Executive Management Group**
Divisional Operational Plans • Annual plans that identify the division's key accountabilities in implementing the department's strategic plan, key strategies and targets. Plans are developed through a process of environmental scanning and reviewing past performance and risks to determine upcoming challenges and new priorities. **Specific Purpose Plans** • Plans that focus on an area of strategic importance to the department to address a particular issue.	**Corporate Risks** • Risks or opportunities that may affect achieving the objectives of the planned outcomes of performance identified through divisional operational plans, specific purpose plans, portfolio plans or programs of change. • At the program level, risks may eventually transition into 'business as usual' upon program completion.	**Divisional Head DD-G**
Portfolio Plans • Plans that support whole-of-government initiatives and departments own strategic agenda.		**Portfolio Manager**
Program Plans • Plans for implementing business strategies, policies and initiatives, or large-scale change, to achieve a desired outcome and benefits of strategic importance. • Involves the management of a group of projects and activities that together achieve the outcomes and benefits.		**Program Manager**
Other cascading plans • This can include planning conducted by branch and work units, regions, schools, TAFE institutes (non-statutory bodies), and projects.	**Operational Risks** • Risks or opportunities that affect plans cascading from the divisional operational plan and achieving the deliverables of projects. • Risks at this level relate to department's systems, resources and processes.	**AD-Gs/EDs** **Regional Directors** **Institute Directors** **Principals** **Project Managers**
Individual Performance & Development Plans • Individual staff *Developing Performance* processes - enable staff to identify how their work contributes to achieving their work unit and departmental objectives.	• When identifying their responsibilities or professional development requirements, staff also need to consider their responsibilities in relation to risk management.	**Individual**

The department has a low appetite for risks relating to health, safety and wellbeing of our students, staff and community and is dedicated to improving risk management within our schools. Risk management in schools assists in decision-making for school personnel and focuses on areas that require attention such as Occupational Health & Safety and Curriculum Activity Risk Management.

This approach:

- leads to informed risk related events for schools
- assists in decision-making, acting as a focus for areas requiring attention, leading to better allocation of resources
- leads to better preparation for worst case scenarios.

Risk governance and accountabilities

Risk governance includes mechanisms that ensure accountability and authority for the management of risk (identifying, assessing, treating and monitoring and reviewing risks); implementation, maintenance and continuous improvement of the department's risk management framework; and providing risk management assurance.

Structures

The department has governance structures that support risk management at the strategic, corporate and operational level:

- **Strategic Structures**
  - *Executive Management Group (EMG)* – sets and reviews the strategic direction, priorities and performance objectives of the department.
  - *Corporate Governance Committees* – support EMG through engagement with a range of strategic agendas.
  - *Audit and Risk Management Committee (ARMC)* –assists in the discharge of the Director-General's financial management responsibilities under the *Financial Accountability Act 2009* and the *Financial and Performance Management Standard 2009* through providing the Director-General with independent audit and risk management advice.
  - *Enterprise Risk Management Committee (ERMC)* – is a sub-committee of ARMC, providing a strategic role in establishing the departmental direction with regards to embedding risk management in all work contexts and levels.
- **Corporate and Operational Structures**
  - Divisional and Program of Change management structures that provide for clear lines of reporting, accountability and responsibility to support appropriate, open and transparent decision making.

Roles and responsibilities

Director-General

The Director-General is the accountable officer under the *Financial Accountability Act 2009* and has ultimate legislative responsibility and accountability for '*establishing and maintaining suitable systems of internal control and risk management'*.

The Director-General is responsible for:

- ensuring systems are in place so that risk owners are held responsible for implementing, monitoring and reporting risks that are within their area of responsibility

- communicating strategic high level inter-agency and State level risks to the appropriate whole-of-government forums
- approving the enterprise risk management and business continuity management frameworks
- considering recommendations from the ARMC in relation to risk management
- advocating for the continual improvement of the department's management of risk.

Executive Management Group

The Executive Management Group (EMG) is responsible for:

- championing a risk management culture and supporting the enhancement of risk management practices across the department
- providing strategic leadership and governance for the department's management of risk, including reviewing effectiveness of internal controls and setting and approving the department's risk appetite and tolerance
- providing oversight of the strategic risks for the department, including reviewing and approving the department's *Strategic Risk Register*, and reviewing the progress of treatment plans for strategic risks that are being managed by divisions
- considering risks that have been escalated by divisions or programs of change including any treatments to mitigate adverse impacts and maximise positive business opportunities
- embedding risk into strategic discussions and analysis occurring at EMG and corporate governance committees.

Senior executives

Deputy Directors-General and Assistant Directors-General (within their area of responsibility) are responsible for:

- ensuring that all employees are aware of and comply with the department's *Enterprise Risk Management Framework 2012-2016*, policy and procedures
- ensuring the effective integration of risk management into planning, reviewing and reporting processes
- leading the risk management practice and ensuring resources and systems for managing risks are established and maintained
- providing oversight of the corporate risks, including reviewing and approving the corporate risks registers, and reviewing the adequacy and effectiveness of the controls and treatments, particularly for high and extreme risks
- escalating corporate risks that are high or extreme to EMG
- considering operational risks that have escalated from within the area of responsibility, including any treatments to mitigate adverse impacts and maximise positive business opportunities
- ensuring that relevant staff are appropriately trained in the process of managing risks
- providing ongoing assurance to the Director-General, EMG and ARMC that risk is being managed effectively.

Senior management

Executive directors, directors, regional directors, principals, TAFE institute directors and managers are responsible in their area of responsibility for:

- managing risks (identifying, assessing, monitoring and reviewing, communicating and reporting) that may impact on their objectives

- providing oversight of the operational risks, including reviewing and approving the operational risks registers, and reviewing the adequacy and effectiveness of the controls and treatments, particularly for high and extreme risks
- considering operational risks that have been escalated within the area of responsibility, including any treatments to mitigate adverse impacts and maximise positive business opportunities
- escalating operational risks that are high or extreme or cannot be managed locally (including risks that require coordination between areas) to line management.

Employees

All employees are required to comply with the department's Risk Management policy and apply risk management processes within their work unit.

Audit and Risk Management Committee

The Audit and Risk Management Committee (ARMC) provides independent audit and risk management advice to the Director-General. The purpose of this committee is to:

- review whether the department has in place a current and comprehensive Framework and associated procedures designed to ensure that the identification and management of risks are effective
- determine whether a sound and effective approach has been followed in managing the department's high/extreme risks
- determine whether a sound and effective approach to the department's business continuity planning arrangements are in place, including whether business continuity and disaster recovery plans have been periodically updated and tested.

Director, Planning, Performance and Risk

Through the Enterprise Risk Management Unit (ERMU), the Director, Planning, Performance and Risk, Governance Strategy & Planning (GSP) is responsible for:

- championing the enterprise risk management function
- developing, implementing, reviewing and continuously improving the department's *Framework*, *Business Continuity Management Framework* and associated policies and procedures
- developing an annual risk management plan and coordinating overall enterprise risk management activities within the department
- managing and coordinating a risk management information system for the department
- collecting and analysing risk data to provide risk information to EMG and ARMC
- assisting EMG to determine the department's risk appetite and tolerance
- providing risk advisory services across the department
- developing the capacity and capability of the department to effectively and efficiently manage risk.

Director, Internal Audit[3]

Within the context of enterprise risk management, the core role of Director, Internal Audit is to provide the Director-General, the EMG and ARMC with objective assurance on the effectiveness of risk management in the following capacity:

[3] Adapted from the IIA Position Paper: The Role of Internal Auditing in Enterprise-wide Risk Management

- giving assurance on risk management processes
- giving assurance that risks are correctly evaluated
- evaluating risk management processes
- evaluating the reporting of key risks
- reviewing the management of key risks.

Enterprise Risk Management Committee

The purpose of the Enterprise Risk Management Committee (ERMC) is to:

- encourage enterprise-wide application of risk management as an integral part of corporate governance, planning and reporting processes
- support the horizontal and vertical integration of risk through open consultation and communication
- provide strategic input into the development, implementation and evaluation of risk programs that support the implementation of the department's *Enterprise Risk Management Framework 2012-2016*
- assist in the monitoring of systemic risk reporting, escalating risk management issues and continuous improvement opportunities to the Audit and Risk Committee.

Other functional oversight areas

A range of central office divisions provide risk oversight and work as key parts of the integrated risk structure to assist in risk identification, analysis, control management and reporting. These areas include:

- Finance (Financial Strategy and Policy)
- Human Resources (Workplace Health and Safety, Fraud and Corruption Control)
- Infrastructure Services (Emergency and Security Management)
- Information and Communication Technology (Information Security)
- Education Queensland (Curriculum Activity Risk Management)
- Corporate Strategy and Performance (organisational performance monitoring and reporting)
- Training and Tertiary Education Queensland (regulatory monitoring and reporting)
- Early Childhood Education and Care (regulatory monitoring and reporting).

Risk system

In addition to the Framework, the risk system consists of components intended to assist the organisation with 'doing risk management right':

- risk management process
- tools – risk registers
- risk reporting.

Risk management process

The risk management process is designed to ensure that risk management decisions are based on a robust approach, assessments are conducted in a consistent manner, and a common language is used and understood across the department. Consistent with AS/NZS ISO 31000, the risk management process consist of seven steps, as outlined in Table 2.

The department's *Risk Management Process* provides a detailed guide to support the effective implementation of the *Enterprise Risk Management Framework*.

Table 2: Steps in the risk management process

Process Step		Description	Purpose
Communication and Consultation		• Involving stakeholders (internal and external) and information sharing throughout the risk management process, vertically and horizontally across the department.	• Context is appropriately defined. • Staff that are involved throughout the risk process understand the basis for decisions and actions required. • Lessons learnt are shared and transferred to those who can benefit from them.
Establish Context		• Understanding the department's objectives and defining the external and internal environment within which the department operates.	• Understand factors influencing the ability to achieve objectives. • Determine boundaries within which the risk management framework operates. • Define risk criteria to ensure risks are assessed in a consistent manner.
Risk Identification	**Risk Assessment**	• Identifying risks, its sources, causes and potential consequences.	• Generate a comprehensive list of threats and opportunities based on those events that might enhance, prevent, degrade, accelerate or delay the achievement of objectives.
Risk Analysis		• Comprehending the nature of the risk and determining the level of risk exposure (likelihood and consequence).	• Provide an understanding of the inherent (level of exposure should controls fail) and controlled risk (level of exposure with controls in place). • Assist with identifying ineffective controls. • Inform risk evaluation and guide risk treatment.
Risk Evaluation		• Comparing the risk analysis with the risk criteria to determine whether the risk is acceptable or tolerable.	• Determine whether the controlled risk is acceptable. • Determine if controlled risks need further treatment. • Identify priority order in which individual risks should be treated.
Risk Treatment		• Selecting one or more options for modifying the risk. • Reassessing the level of risks with controls and treatments in place (residual risk).	• Identify treatments for risks that fall outside the department's risk tolerance. • Provide an understanding of the residual risk (level of risk with controls and treatments in place). • Identify priority order in which individual risks should be treated, monitored and reviewed.
Monitoring and Review		• Determining whether the risk profile has changed and whether new risks have emerged. • Checking control effectiveness and progress of the treatment plan.	• Provide currency of risk information • Identifying emerging risks. • Provide feedback on control efficiency and effectiveness. • Identify whether any further treatment is required. • Provide a basis to reassess risk priorities. • Capture lessons learnt from event failures, near-misses and success.

Please refer to *the department's risk management process* for more information.

Tools – risk registers

The risk register enables staff to document, manage, monitor, review and update strategic, corporate and operational risk information. Risk register reporting allows management to monitor and review risks in alignment with the strategic plan, division's operational plans, programs of change and other cascading plans.

Information from the risk management process is recorded, reported and monitored using the department's risk register. The department has two ways to record risks:

- **ERA risk register** – an online risk management tool, to assist staff in recording risk information within their areas of responsibility in a near real-time environment.
- **Offline risk registers** – for staff who cannot access ERA online.

Risk reporting

As there is no one single risk report that meets the decision-making needs of an organisation, risk reports are to be tailored by the accountable area to support management decision making during the planning and review processes.

Risk reports draw information from the risk registers and, depending upon the requirements, may include:

- a demonstration of the link between objectives and risks
- priorities, based on the risk rating, accompanied by information on key controls and treatments needed to modify the risk
- risks that are getting worse, success of treatment plans and risks that require additional attention
- new risks that may still need to be fully considered and understood
- potential areas that require urgent attention
- main areas of exposure
- systemic control analysis
- untreated risks and risk treatments that are overdue
- risk owners.

In addition to the risk reporting conducted by the accountable areas, ERMU report on corporate and strategic risks to the Executive Management Group at least biannually.

Tools – building risk capability

A range of training and development tools are available to build staff awareness and develop skills in 'doing risk management right' and 'doing the right risk management'. This increased awareness and understanding provides staff with greater self-confidence and willingness to take responsibility for the management of risk across the department.

Risk management capacity building is tailored according to the specific needs of the business area. To facilitate this the department uses an experiential learning approach and has developed various training and development tools and products that business areas are able to access to improve their risk management capability.

Related policies and procedures

Departmental policy instruments

The department's policies provide a key mechanism to enable staff to manage risks.

The department's *Policy and Procedure Register* is the central location for policies, procedures, guidelines and other administrative instructions and directives.

Business continuity management

Business continuity management is an integral part of the department's *Enterprise Risk Management Framework.*

Business continuity focuses on the risk of failure to deliver critical services in the event of disaster or crisis. The department's *Business Continuity Management Framework* aims to build high level resilience in all departmental sites and services when facing major adverse events. It outlines the roles, responsibilities and management required to prevent, respond to, continue during and recover from a disruption-related risk, with the safety of staff, students and other community members always its first priority.

Health, safety and wellbeing

The *Workplace Health and Safety Act 2011* and the *Workplace Health and Safety Regulation 2011* provide the foundation for the integration of health, safety and wellbeing into the department's core business operations and is a key focus for the department in delivering quality educational and training outcomes in safe and supportive working and learning environments. In support of this, the department has produced the following strategic documents:

- *Health, Safety and Wellbeing Policy Statement* – outlines the department's commitment to achieving its health, safety and wellbeing targets
- *Health, Safety and Wellbeing Management Framework 2011-2015* – identifies the current health, safety and wellbeing priorities; and charting the responsibilities all staff and others have in achieving those priorities
- *Health, Safety and Wellbeing Strategic Plan* – outlines the expectations and performance standards for achieving the health, safety and wellbeing priority areas

To support these three strategic documents, the department has developed and maintains a suite of operational procedures for health, safety and wellbeing. These procedures form part of the *Policy and Procedure Register* and outline the responsibilities staff have to address specific issues in their workplaces (such as Curriculum Risk Management, Infection Control, and Staff Rehabilitation).

Curriculum Activity Risk Management

The department is committed to the health, safety and wellbeing of students, staff and others involved in all curriculum activities conducted at schools or other locations. To support effective curriculum activity risk management in schools, the department has in place:

- *Managing Risks in School Curriculum Activities Procedure* – outlines the responsibilities that regional directors, principals, teachers and others have in managing the hazards and risks associated with school curriculum activities
- *Curriculum Activity Risk Assessments* (CARAs) – a number of activity-specific guidelines outlining risk level, minimum recommendations (supervision, qualifications, equipment), and identified hazards and control measures.

Fraud and corruption

The department's *Fraud and Corruption Control Policy* (FCCP) incorporates best practice guidelines as detailed in the Crime and Misconduct Commission's (CMC) *Fraud and Corruption Control – Guidelines for Best Practice 2005*.

This policy is an integral part of the department's risk management framework. It tasks all managers with responsibility for the prevention, detection and reduction of business risks or exposures. These factors underpin our zero tolerance approach, with the desired outcome being the prevention of all fraud related incidents within the department. The department's fraud and corruption strategy will at all times ensure the protection of public property, information, revenue, expenditure, and the rights of organisations and individuals.

Information security

The objective of information security management is to ensure that information is protected to ensure its availability, confidentiality and integrity. This ensures the effective provision of government services in compliance with legislation and the Queensland Government *Information Standard 18: Information Security (IS18)*. All staff are responsible for ensuring the safety of our information and electronic systems. The department's *Information Security Management Policy* provides a set of guidelines for maintaining information security, while its security procedure *Maintaining the Security of Department Information and Systems* informs staff of the requirements to protect and secure the department's information and computer systems.

Implementing risk management

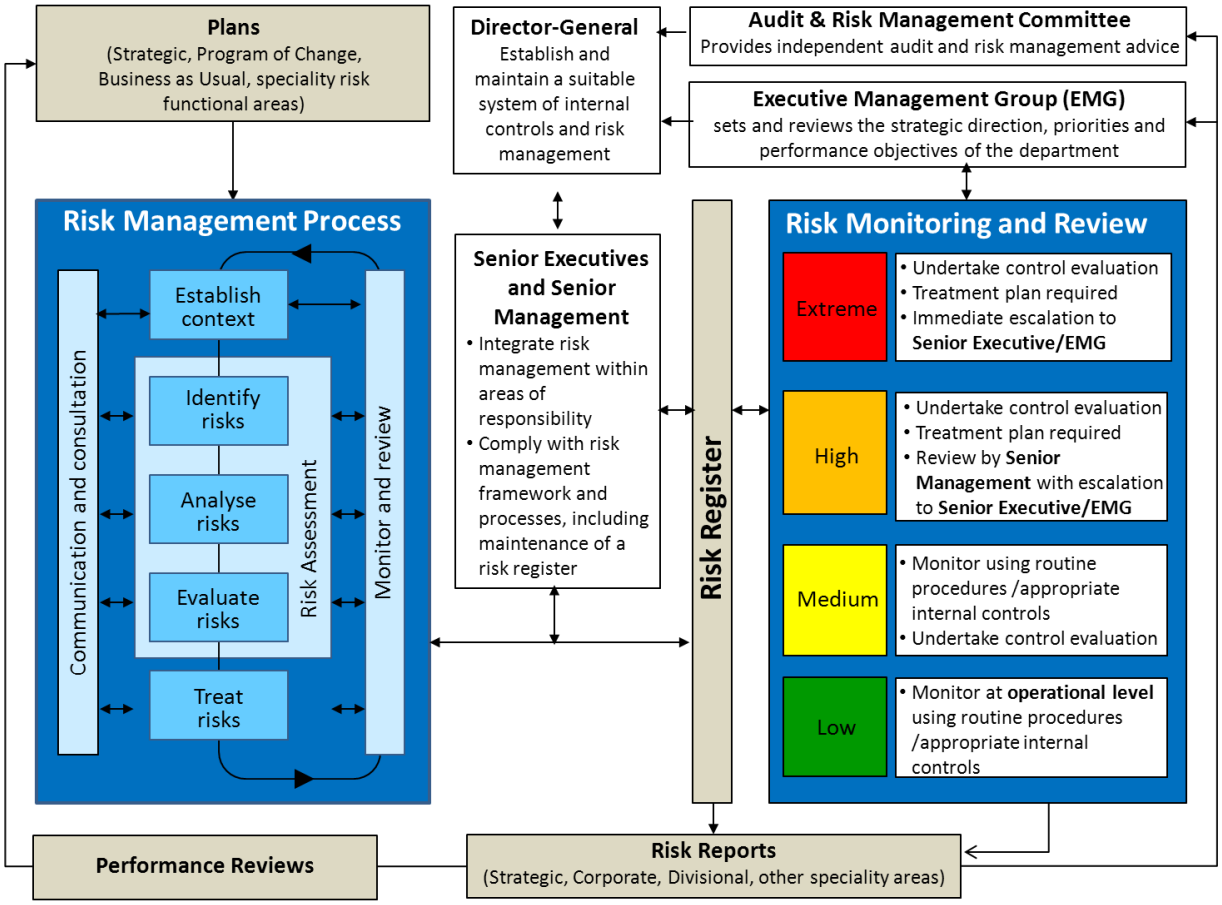
Risk management should be implemented by ensuring that the risk management process is applied at all relevant levels and functions of the organisation as part of its practices and processes.

Risk management - Principles and guidelines (AS/NZS ISO 31000:2009)

The department's risk management process

Figure 2 provides an overview of how the steps in the department's *Enterprise Risk Management Process* (ERMP) interrelate to the department's planning, reviewing and reporting cycle; risk governance components of the Framework; and the actions required from the risk monitoring and reviewing process.

Figure 2: Department of Education, Training and Employment Risk Management Process: An overview



The ERMP has been designed to provide the '*risk owner',* (the person that has been given the authority and accountability to manage a particular risk[4],) the necessary resources to ensure that risk management decisions are based on a robust approach, assessments are conducted in a consistent manner, and a common language is used and understood across the department.

As part of the ERMP, the **Risk Consequence Table** provides risk owners with a tool for considering the severity of the consequences of risks.

[4] Adapted from Australian Standards for Risk management - Principles and guidelines (AS/NZ ISO 31000:2009)

The Risk Matrix expresses the department's tolerance for risk, by making a determination as to the level of risk that is acceptable, based on the combined likelihood of the risk occurring and potential consequences of the risk. This will dictate the points at which risks need to be escalated.

Monitoring, review and continual improvement of the Framework

Risk management should support organisational performance through indicator based risk review, progress measurement against the risk management plan, risk framework appropriateness and effectiveness and risk reporting.

Continual review of the framework should be based on results of monitoring and reviews, with decisions relating to how the framework, policy and plan can be improved to support management of risk and an improved risk management culture.

Risk management - Principles and guidelines (AS/NZS ISO 31000:2009)

Continuous improvement is strategically integrated with the department's corporate objectives to ensure that the department continues to evolve towards best practice.

Governance Strategy and Planning (GSP) is responsible for continual improvement of the department's risk management, including the *Enterprise Risk Management Framework*.

Some of the processes that support continuous improvement and review of the Framework include:

- regular assessment of the quality of risk management processes and artefacts prepared by business areas to identify opportunities for improvement
- a baseline and ongoing risk management culture survey data to inform improvement, communication and training requirements
- regular reviews of models, frameworks, and standards used in other organisations and jurisdictions to ensure that our Framework continues to reflect contemporary best practice
- ongoing training and development for ERM team staff to ensure that the team is equipped with a sound knowledge and skills base
- inclusion of, and measurement against, performance measures relating to the department's performance with regard to risk management and other key governance processes in Corporate Strategy and Performance's operational plan.

GSP will review the Framework annually and will work with divisions to ensure that the Framework and associated business processes continue to meet local needs as risk management matures and improves.

Appendix 1

The Framework is underpinned by legislation, Australian and International Standards and a number of evolving best practice standards and guidelines:

1. The *Financial Accountability Act* 2009
2. Standards Australia, AS/NZS ISO 31000:2009 *Risk management – Principles and guidelines*
3. The State of Queensland (Queensland Treasury) *A Guide to Risk Management*, July 2011
4. The State of Queensland Department of the Premier and Cabinet, *Risk Management Guide*, May 2011
5. Victorian Managed Insurance Authority (VMIA), *Risk Management: Developing & Implementing a Risk Management Framework*, March 2010
6. Department of Treasury and Finance (Vic), *Victorian Government Risk Management Framework*, March 2010
7. HM Treasury, *The Orange Book; Management of Risk – Principles and Concepts*, October 2004
8. HM Government, *Risk: Good Practice in Government*, March 2006

The Framework is supported by departmental procedure:

1. Enterprise Risk Management (http://ppr.det.qld.gov.au/corp/governance/Pages/Risk-Management.aspx)

   Supporting documents:

   - *Enterprise Risk management framework 2012-2016*
   - *Enterprise Risk management process*
   - *Fact sheets*
   - *ERA Risk Register*
   - *Offline Risk Register Template*
   - *ERA Handbook*