DET Risk Management Framework

June 2016

Published by the
Department of Education and Training
Melbourne
June 2016

Authorised by the Department of Education and Training,
2 Treasury Place, East Melbourne, Victoria, 3002.
This document is also available on the internet here

Secretary's Message

To meet the expectations of the community, and to achieve our strategic objectives, we must be prepared for risk. Risk is inevitable and part of the work we undertake. It is not something that can or should be avoided, as through the appropriate identification and management of risk, we will create opportunity. We need to be productive, innovative and efficient; anticipating and managing the uncertainties that could positively or negatively affect the delivery of our services, maximising our ability to realise opportunities and improve educational outcomes for Victorians.

To do this, we have in place a risk management framework that informs our decision making and resource prioritisation and supports the achievement of objectives.

The Framework signals my commitment to a systematic and integrated approach to the proactive management of risks, both threats and opportunities, to improve decisions and outcomes across the Department.

Risk management is everyone's responsibility and must be integrated into all planning and implementation activities. Consistent application of the Framework will help us to build a proactive risk culture that maximises opportunity whilst minimising negative outcomes.

The Framework applies to all parts of the department including schools, and I invite you to familiarise yourself with the framework documents and tools, and access the range of helpful resources that we have to support you.

Gill Callister, Secretary

1. Introduction

1.1 Purpose of the risk management framework

The Department of Education and Training (DET) (the Department) recognises that risk management is integral to achieving our vision, mission and goals. Risk management maximises the ability to deliver on departmental objectives, promotes sound decision-making for resource allocation and investment, works to safeguard student and employee wellbeing and contributes to meeting the Victorian community and Government expectations for accountable and responsible use of public finances and resources. The Risk Management Framework also intends to provide and operate within an environment of continuous improvement and ongoing business excellence, enhancing the Department's focus on learning and development.

The DET Risk Management Framework (the Framework) provides the outline of DET's approach to risk across the business, and the implementation of this framework ensures that the Department embeds risk management in its business processes, and that the risks will be managed effectively and efficiently to deliver outcomes and objectives. The Framework will also be used to inform the development of new, and refinement of existing guides, tools and training.

1.2 Scope

The Framework applies to all elements of the Department, including:

- central and regional offices
- all Victorian government schools.

Other entities within the portfolio can use this as a guide.

1.3 Defining risk and risk management

Risk is the 'effect (positive or negative) of uncertainty on objectives'.

Risk management is the identification, analysis, assessment, and prioritisation of risks to the achievement of objectives. It is the coordinated allocation and prioritisation of resources and investment to minimise, monitor, communicate and control risk likelihood and/or impact, or to maximise the realisation of opportunities. **Risk management is an integral part of good management practice.**

1.4 Goals of the Framework

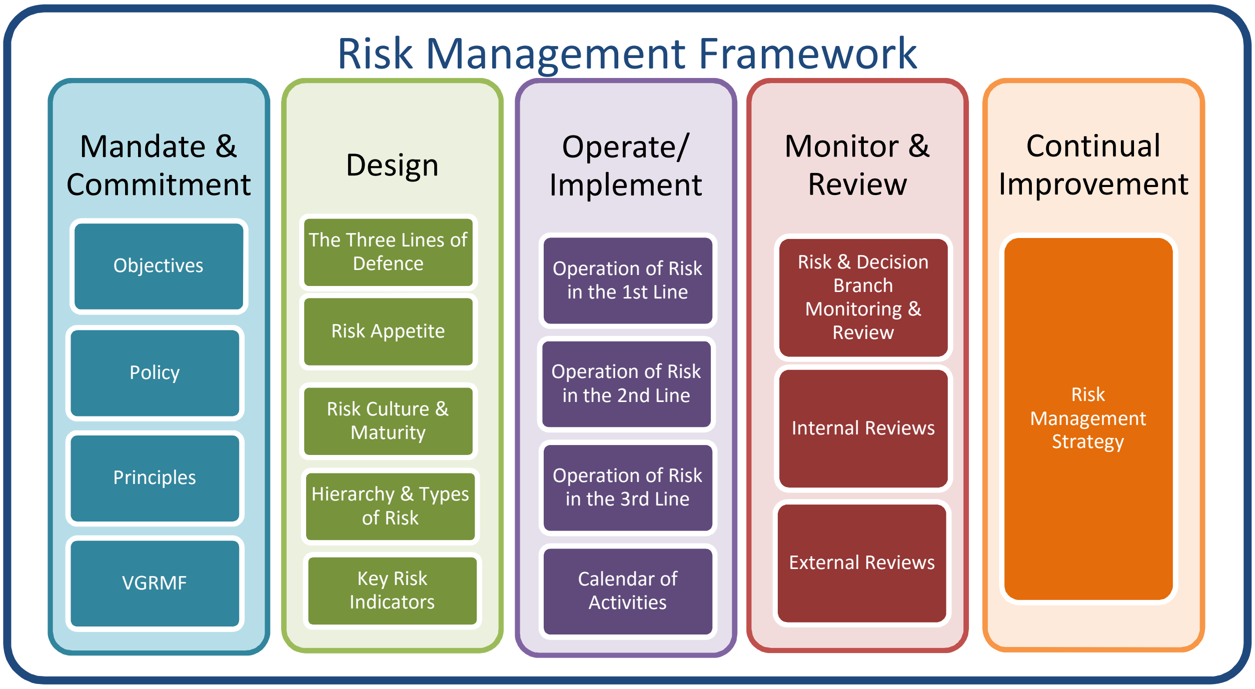
Through implementation of the Framework, the Department aims to:

- integrate risk management into the culture of the organisation
- embed risk management into all planning activities and business decision making processes including informing investment and resource allocation to assist in the delivery of outcomes
- ensure that systems are in place to track and report upon existing and emerging risks to the achievement of the Department's objectives
- introduce a standardised approach to the management of risk across the Department
- increase understanding and awareness, provide guidance and clarify accountability and responsibilities in relation to risk
- provide simple guidelines for the development, implementation and management of risk at various level
- provide an appropriate process to give rigour to the risk attestation statement within the Department's annual report.

2. DET Risk Management Framework

The Framework has five components, each with a number of sub-components outlined in Figure 1.

Figure 1 – DET Risk Management Framework



2.1 Mandate and commitment

DET is committed to strong and sustained risk management to ensure informed and transparent decision making and prioritisation. This mandate will ensure the ongoing effectiveness of risk management in the Department.

As set out at the beginning of this document, the Framework has the full support of the Secretary and the Executive Board.

2.1.2 Objectives of risk management

Embedding risk management at all levels of the Department is designed to:

- increase the likelihood of the Department achieving objectives and realising opportunities
- ensure impartial and properly evaluated risk based decisions are made
- implement cost effective actions to reduce risks
- actively manage risk in accordance with best practice to ensure that it is reduced to an acceptable level
- ensure the Department anticipates and takes appropriate action to manage risks
- improve planning at a group, division, region and school level
- prepare for the future
- improve organisational resilience
- improve stakeholder confidence and trust
- comply with relevant legal and regulation requirements.

2.1.3 DET risk management policy statement

Management of risk is the responsibility of all staff.

The effective management of risk is central to the continued enhancement of quality outcomes for the Department. By understanding our risks, we can develop effective strategies that will enhance the Department's ability to support Victorians to build prosperous, socially engaged, happy and healthy lives.

Throughout the Department we will adopt a structured and consistent approach for recognising, understanding and responding to risk. This approach is consistent with the Australian/New Zealand standard for risk management ISO 31000:2009 and the Whole of Victorian Government Risk Management Framework.

We operate under one Risk Management Framework that enables the management of risk to become integrated into all our business activities and decision making processes.

Governance of the risk management practices will be assured through regular reporting of our risk management performance to the Executive Board and Portfolio Audit and Risk Committee (PARC). Each year, the Secretary is required to attest, as verified by the PARC that the Department understands, manages and controls key risk exposures.

In the interests of standardisation across the Portfolio, those statutory authorities which do not have their own risk management framework are encouraged to adopt and utilise the Department's framework.

2.1.4 DET risk management principles

The Department is committed to implementing a proactive and targeted approach to risk management which is based on the following key principles found within ISO 31000:2009 Risk management – Principles and guidelines:

a) *Risk management creates and protects value.*
Risk management contributes to the demonstrable achievement of DET's objectives and improvement of performance in, for example, human health and safety, security, legal and regulatory compliance, public acceptance, environmental protection, product quality, project management, efficiency in operations, governance and reputation.

b) *Risk management is an integral part of all DET organisational processes.*
Risk management is not a stand-alone activity that is separate from the main activities and processes of the organisation. Risk management is part of the responsibilities of management and an integral part of all organisational processes, including strategic planning and all project and change management processes.

c) *Risk management is part of decision making.*
Risk management helps decision makers within the Department reach informed conclusions, select appropriate actions and discriminate between other courses of action.

d) *Risk management explicitly addresses uncertainty.*
Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and best way it can be addressed.

e) *Risk management is systematic, structured and timely.*
A systematic, timely and structured approach to risk management contributes to efficiency and to consistent, comparable and reliable results.

f) *Risk management is based on the best available information.*
The inputs to the process of managing risk are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts and expert judgement. However, decision makers should inform themselves of, and should take into account, any limitations of the data or modelling used or the possibility of divergence among experts.

g) *Risk management is tailored.*
Risk management is aligned with the Department's external and internal context and risk profile.

h) *Risk management takes human and cultural factors into account.*
Risk management recognises the capabilities, perceptions and intentions of external and internal people who can facilitate or hinder achievement of the organisation's objectives.

i) *Risk management is transparent and inclusive.*
Appropriate and timely involvement of stakeholders and, in particular, decision makers at all levels of the organisation, ensures that risk management remains relevant and up-to-date. Involvement also allows stakeholders to be properly represented and to have their views taken into account in determining risk criteria.

j) *Risk management is dynamic, iterative and responsive to change.*
Risk management continually senses and responds to change. As external and internal events occur, context and knowledge change, monitoring and review of risks take place, new risks emerge, some change, and others disappear.

k) *Risk management facilitates continual improvement of the organisation.*
The Department should develop and implement strategies to improve the risk management maturity alongside all other aspects of the organisation.

2.1.5 Victorian Government Risk Management Framework

The Victorian Government Risk Management Framework (VGRMF) describes the minimum risk management requirements agencies are required to meet to demonstrate that they are managing risk effectively, including inter‑agency and state significant risk. It outlines the role and responsibilities of an agency's responsible body. The VGRMF adopts ISO 31000:2009 Risk management – Principles and guidelines, which provides a generic, internationally accepted basis for best practice risk management.

The VGRMF is mandated by the Standing Direction of the Minister for Finance 4.5.5 – Risk Management Framework and Processes and provides high level information for agencies and the responsible body.

The VGRMF was updated in 2015. It incorporates existing mandatory requirements relating to risk and insurance management practices and policies and streamlines the annual attestation requirements.

Victorian Government Risk Management Framework document

2.2. Design of risk management within the Department

The design of Risk management at DET is based on the three lines of defence model. This outlines the ownership, accountabilities, resources and governance for risk management activities within the Department.

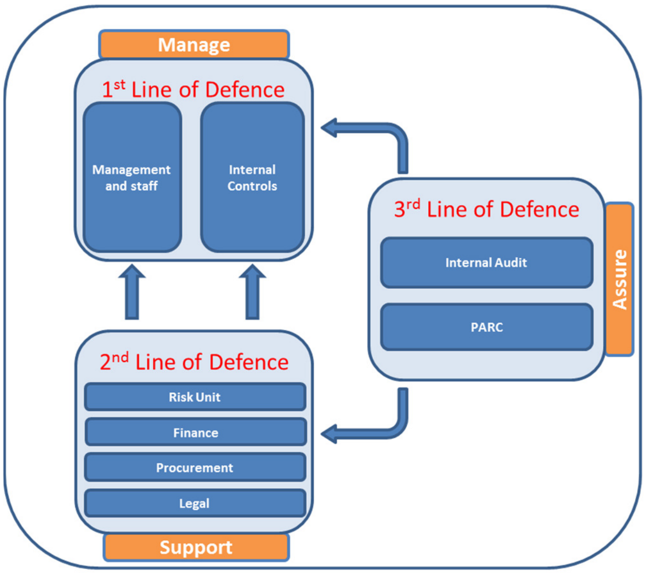
2.2.1 The three lines of defence

The three lines of defence model illustrates the layers that provide rigour to the management of risks to the Department's objectives. It formalises the relationship and accountability between the three lines (outlined in Figure 2).

The three lines are:

First Line -	Functions that own and **manage** risks.
Second Line -	Functions that oversee and **support** the management of risk.
Third Line -	Functions that provide independent **assurance** over the management of risk.

Figure 2 - Three lines of defence for DET



2.2.1.1 The First Line – Functions that own and manage risks

Executive officers, principals, managers and all staff are accountable for the management of risk within their areas of responsibility and related to the decisions they make (or do not make – as risk levels may increase when decisions are avoided). They also are responsible for implementing corrective actions to address process and control deficiencies.

Ministers

The ministers set the objectives and policy framework for the Department. As the lead minister, the Minister for Education has accountability for the effectiveness of risk management in schools through the *Public Administration Act 2004.*

Executive Board (including Secretary)

The Department's Executive Board is accountable for effective risk management in the Department and for ensuring that the decisions they make are risk-based. The Secretary also completes the annual risk attestation statement.

Governance Committees

The primary purpose of committees is to make decisions or provide advice to the Executive Board and the Secretary. Committee membership should possess relevant and appropriate capability and diversity to support effective decision-making. Each Governance committee should utilise existing risks to help prioritise significant projects to be included in its workplan.

Governance committees are expected to escalate or refer to the Executive Board for a decision all significant risks or issues that will impact the delivery of objectives and outcomes.

Executive Officers

Executive officers are accountable for identifying, assessing, prioritising and effectively managing risks within their area of responsibility. Deputy Secretaries, Executive Directors and Regional Directors also complete annual risk management sub-attestation statements.

Principals

Principals are accountable for identifying, assessing, prioritising and effectively managing risks within their area of responsibility.

Managers

Managers are accountable for identifying, assessing, prioritising and effectively managing risks within their area of responsibility.

All other staff – including VPS, teachers and school support staff

All staff are responsible for identifying risks within their area of responsibility and escalating them to relevant body or person.

2.2.1.2 The Second Line – Functions that oversee and support risk management

Management establishes risk management and support functions to help build and/or monitor the first line of defence risk management practices.

Risk and Decision Branch

The Risk and Decision Branch (RDB) is responsible for risk management strategic direction, guidance, assurance, improvement and verification. The Chief Risk Officer (CRO) is responsible for assessing the adequacy of risk management and risk management plans across the Department, informing the Executive Board of that assessment at least annually.

Risk Coordinators

Given that accountability for the management of risk lies with executive officers and managers, a network of risk coordinators has been established to support the bi-annual operational risk review process within the central office and regional functions. These are nominated staff who act as the liaison between the RDB and the divisions/regions. They facilitate discussions and coordinate formal responses to risk requests on behalf of their division. They also provide risk advice to project teams.

Support Functions

The Department has support functions that provide policies and advice to first line management teams and include: Finance, Human Resources, Integrity, Procurement, Legal, Communications, Information Management/Technology and Business Planning.

The responsibilities of these functions, including the RDB, vary on their specific nature, but can include:

- developing and supporting management policies, defining roles and responsibilities, and setting goals for implementation
- identifying known and emerging issues and risks
- identifying shifts in the organisation’s implicit risk appetite
- assisting management in developing processes and controls to manage risks and issues
- providing guidance and training on risk management processes
- facilitating and monitoring implementation of effective risk management practices by operational management
- alerting operational management to emerging issues and changing regulatory and risk scenarios
- monitoring the adequacy and effectiveness of internal control, accuracy and completeness of reporting, compliance with laws and regulations, and timely remediation of deficiencies
- implementing and managing second line of defence controls.

Executive Board – Oversight

In addition to its first line accountabilities, the Executive Board will provide strategic leadership and governance for risk management and promote the implementation of risk management across the Department.

School Councils

School councils are the key governing body for schools. Their accountability includes monitoring and reviewing the effectiveness and currency of risk management, compliance and reporting systems and notifying the appropriate bodies of known risks requiring escalation.

2.2.1.3 The Third Line – Functions that provide independent assurance

This line provides a level of independent assurance that the risk management and internal control framework is working as designed.

Internal Audit

The overarching mission of internal audit is to enhance and protect organisational value by providing risk-based and objective assurance, advice and insight. Internal audit provides independent and objective assurance to the Secretary that the Department's financial and operational controls, designed to manage organisational risks and support the achievement of objectives, are operating in an efficient and effective manner.

Internal audit provides the Department's Portfolio Audit and Risk Committee and senior management with assurance based on the highest level of independence and objectivity. This level of independence is not available in the first or second lines of defence.

The objectives and scope of the internal audit function is documented in the Internal Audit Charter.

Portfolio Audit and Risk Committee (PARC)

The PARC provides advice on the risk management framework and tools. The PARC charter outlines that it shall:

- develop a 'whole-of-enterprise' understanding of risks to the portfolio and the control mechanisms in place to control those risks
- review the portfolio's risk management framework, and adequacy of strategic and business risk management
- review the adequacy and effectiveness of portfolio business continuity management arrangements, including disaster recovery and emergency management planning and testing
- review whether appropriate policies and processes are in place for fraud control prevention, detection, reporting, response and investigations
- review whether management's approach to maintaining an effective internal control framework is sound and effective
- recommend to the Secretary whether the risk attestation may be signed.

To support the Secretary's risk management compliance attestation, the RDB provides PARC with appropriate risk management reports including:

- quarterly strategic risk reports – after endorsement by the Executive Board
- a profile of the Department's operational risks and key operational risks (bi-annually)
- a report on the annual electronic internal compliance certification and attestation process.

PARC reviews the Portfolio Audit Plan to determine whether risks or control system weaknesses or gaps warrant reprioritisation of the plan.

2.2.2 Risk appetite

Risk appetite is an articulation of the type and amount of risk that an organisation is prepared to accept or avoid in the pursuit of its objectives. It is about the level of risk exposure the Department is prepared to accept or could justify if the risk materialised. It is about the effort and resources the Department expends to manage a risk compared to the potential cost or alternatively, it is about how much we are prepared to actively put at risk in order to pursue opportunities.

Where risks relate to fraud and corruption, child safety/abuse, and legislative and regulatory non-compliance, the Department's appetite for risk is zero. Conversely the Department has a much higher appetite for risk in relation to elements such as policy innovation and invention.

In practice the Department's overarching attitude to risk is that it must be identified and assessed, and that decisions on risk appetite are devolved and provided through the acceptability chart and consequence guide.

This means that decisions on acceptability or tolerance for risk, and pursuit of opportunities, will be context based and dependent upon the responsibility and accountability of executive officers, principals and managers in order to enable them to pursue the Department's objectives.

2.2.3 Risk culture and maturity

Our culture echoes how we approach our effort and interrelate with each other, and is driven by our values and behaviours. Culture influences how we make choices, solve difficulties, create and innovate, and how we work together and thrive as a department. Risk culture refers to the behaviours that lead to how every person identifies and manages risk. Risk culture is an element of the department's overall culture.

A strong risk culture does not mean a culture of risk aversion. The Department seeks to innovate and deliver services to "give every Victorian the best learning and development experience, making our state a smarter, fairer and more prosperous place". This means embracing risk in a considered manner.

To realise the most from the Risk Management Framework, DET aims to be an organisation that has a risk culture in which employees at all levels think about managing risks as part of "how things get done around here" in their day-to-day business. The Department's risk culture needs to be driven, and enhanced, by all managers and individuals taking a proactive approach to managing risk in order to maximise the possibility of achieving objectives.

A mature risk management culture will appreciate that effort expended in risk management should be proportional to the magnitude of risk. Risk management activities must be integrated with all planning and decision-making activities and operations across the Department, in central and regional offices, schools and other facilities. As such, all staff are responsible for managing risk in their areas of responsibility in their day-to-day business, with the senior executives leading the way as risk champions.

Schools, in particular are encouraged to work with the broader school community, including school council, service providers, students and parents to facilitate a risk aware culture. Differing attitudes, demographics and interests need to be considered when considering the desired risk culture of a school and subsequently the way risk will be managed.

2.2.4 Hierarchy and types of risk

The department classifies risk into three distinct categories: strategic, operational and project risk. There is a hierarchy inherent in these categories. There are also inter-agency and state significant risks that operate within this hierarchy.

2.2.4.1 Strategic risk

Strategic risks are those which could impact on the achievement of the DET strategic intent. They may impact across multiple groups/areas or the Victorian community. They are key matters for the Executive Board and often affect the whole business, rather than just an isolated area. They may be long term and emergent in nature. They are identified and owned by the Executive Board, who monitor the risk exposure and the status of controls and treatments, and agree changes in risk exposure. The review of strategic risk informs strategic planning and resource prioritisation at a departmental level. Activities to treat strategic risks are usually delegated to groups/divisions/regions to deliver. Risk treatment plans are actively monitored by nominated risk leaders and reported to the Executive Board and PARC quarterly.

Strategic risks include one or more of the following key attributes:

- significant risks that affect the longer term interests of the Department and the community
- key direct and portfolio significant risks to achieving DET's overall strategic priorities and outcomes and/or risks that might otherwise influence choices around our strategic priorities, initiatives and resources
- risks that require significant co-ordination between different parts of DET and/or or with external stakeholders

- risks that arise externally which could significantly impact DET
- execution risks that could arise from pervasive aspects of our internal environment.

2.2.4.2 Operational risk

Operational risks are those which could impact on the ability of schools, groups, divisions or regions to deliver on day-to-day or service delivery objectives. Principals and executive officers are accountable for identifying, evaluating and managing operational risks and must ensure appropriate controls and/or treatment plans are implemented and reviewed. Group executive teams discuss and share their risks and escalate key operational risks to the Executive Board for review and to inform investment and resource prioritisation.

2.2.4.3 Project risk

Project risks impact on the achievement of individual projects or programs of work. They may be identified at all stages of the project or program lifecycle. Project and program managers are expected to implement appropriate risk management processes to ensure the effective and efficient delivery of the project and prioritisation of project resources.

While identifying project risks, it is also about understanding the risks we must take to achieve project objectives. A review of the risks to a project should be a standard agenda item for regular project board meetings, to ensure that decisions made are informed by the risks to the objectives.

2.2.4.4 Inter-agency and state significant risks

In addition to strategic, operational and project level risks, DET is also required to manage risks that extend beyond the effective management of DET's specific risks. Consideration is also required to the identification and communication of inter-agency and state significant risks. This is increasingly important under a system of joined up government where the focus is on outcomes which may require a whole of government approach to risk management.

All business areas should consider, identify and manage inter-agency and state significant risks as part of their risk management activities. Identification of inter-agency and state significant risks is to include identification of the other agencies that are critical in managing these risks and how action is to be coordinated. The Department is expected to work collaboratively with other agencies so that shared risks are managed effectively. Agencies are responsible for ensuring that state significant risks are communicated to and considered by decision makers at the appropriate level of government.

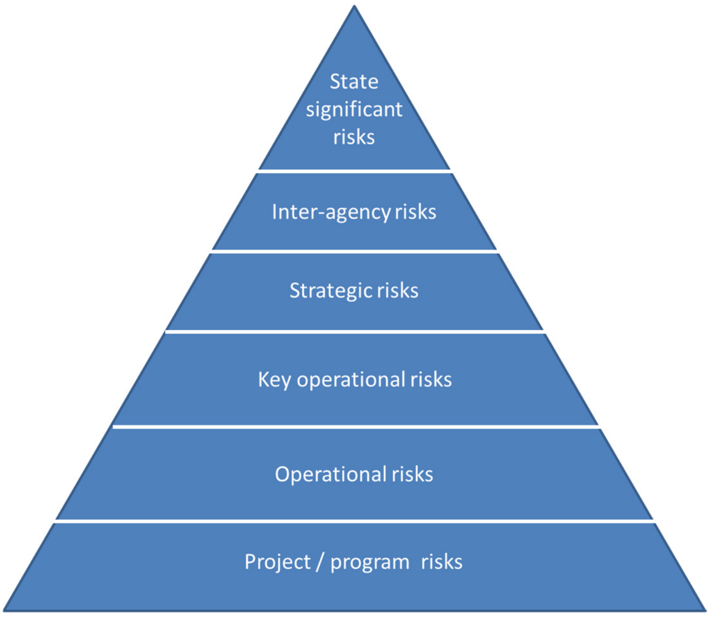
The Victorian Government Risk Management Framework (VGRMF) 2015 identifies inter-agency and state significant risks as indicated in Figure 3.

- **Inter-agency risks** are risks shared by two or more agencies that require coordinated management by more than one agency and may include systemic risks. The responsibility for managing an inter-agency risk is shared by all of the relevant agencies and will benefit from a coordinated response where one agency takes a lead role.
- **State significant** risks are risks where the potential consequences or impacts of the risk on the community, the government and the private sector are so large are to be of state significance. A state significant risk can be the extension of an existing agency risk which, beyond a certain threshold, becomes severe enough to have state wide implications or it could be the aggregation of many agency specific risks.

2.2.4.5 Interrelationship of risks

Strategic risks are identified and allocated to divisions or regions for management as a result of discussions at Executive Board ("top down" process), with significant operational and project risks escalated for consideration by the Executive Board through risk identification from individual groups, regions, divisions or projects ("bottom up" process).

Figure 3: categories of risks



2.2.5 Key risk indicators

Key risk indicators (KRI) are measures or pointers used to observe possible changes in risk situations or new emerging risk affecting the Department's outcomes, objectives and strategies. They deliver initial cautions to proactively detect the prospect of a future adverse impact. Early warning allows management to be in an improved position to manage actions that may happen in the future, in a timely and considered basis.

Most indicators are not universal, rather they are often specific to individual businesses or processes. The opportunity is to implement KRIs in such a way as to ensure uniformity, relevance, transparency and comprehensiveness. Readily understood and communicated key performance indicators and risk indicators are developed and reviewed to monitor performance against the business plan and to monitor changes in the exposure to strategic risks. The Department does not currently utilise KRI's, but as the Department risk maturity improves will be embedded into risk management processes.

2.3. Operation/implementation of risk management

The operation/implementation component outlines how risk is conducted practically at DET. This outlines the processes and procedures used by the first, second and third lines to plan, manage and report on risks to the achievement of objectives.

2.3.1 Operation/implementation in the first line

For management and staff, the risk processes form an integral part of planning and day-to-day management and require regular reporting.

2.3.1.1 Risk in DET planning processes

Risk management is an integral component of effective corporate and business planning. Within DET, risk management is fully integrated with the department's planning cycle. Key risks associated with the achievement of objectives established through groups and their supporting divisions and regions must be identified and discussed as part of forward planning discussions, when developing business plans, and as a matter of course throughout the year.

Future deliverables and objectives must ensure appropriate allocation of resources, time and budget to the identification and treatment of risks. Risk treatment plans must be fully integrated and included in business plans.

At the project level, planning for and implementing the Risk Management Framework must be considered in project planning documents, milestones and gateways.

Risk management at the strategic, operational and project level is an ongoing process throughout the year. Key features of the risk management and annual planning processes are:

- the DET **Strategic Plan**, establishing the Department's corporate objectives, is a four year forward looking plan that is reviewed on an annual basis. The Department can also prepare an **annual plan** which highlights areas of focus for the Department. The strategic risk management process is an essential element in the analysis of the Strategic Plan and the annual Plan.
    - The Executive Board is responsible for the identification and management of the strategic risk profile, and ensuring all strategic risks are considered and integrated as part of the Department's planning.
- **Business Plans**, defining the strategies and actions that will be employed to deliver the department's group and divisional objectives, are completed yearly. The **operational risk management** process influences group, divisional and regional objectives and strategies, and increases the likelihood of success.
    - Each group is required to develop a business plan that details all of their programs, actions and tasks for the financial year. Business plans include a risk management plan, which addresses any risks to the delivery of strategies and actions. As part of good performance management practice, groups are encouraged to regularly review their progress against their plans.
    - Throughout the year, groups, divisions and regions identify actions and tasks that contribute to the delivery of DET's strategies. These are detailed in the operational plans to mitigate operational and project risks.
- the **budget and resource allocation** process is driven by the delivery of the outcomes and objectives detailed in the DET strategic and business plans.

For schools, when developing their **School Strategic Plan (SSP)** and **Annual Implementation Plan (AIP)** consideration should be given to the operational and strategic risks facing the school in the achievement of their goals and objectives. The identification of these risks should assist in the setting of actions to achieve their implementation and strategic plan objectives.

2.3.1.2 Management of risk (the risk process)

The risk management process is the approach and mechanisms by which the Framework shall be implemented and delivered at all levels and functions of the department. This is the process that groups, divisions, regions and schools should be utilising when seeking to maximise the chances of achieving strategic, operational or project objectives and outcomes by undertaking a structured risk assessment.

The key components of the process are:

1. **Establish the context** - understanding the environment in which the department seeks to achieve its objectives. It includes planning the remainder of the risk management process and may involve the use of tools such as SWOT analysis, a PESTLE view, brainstorming etc.

2. **Risk identification** - determining what, where, when, why and the risks might arise, and the consequences on the department ability to achieve its objectives and the sources of the causes.

3. **Risk analysis** - is based on a detailed understanding of the risk obtained from the process so far. Identification and consideration of the effectiveness of controls should be undertaken. The risk is described using the risk matrix and standard risk terminology of likelihood and consequence to determine the risk rating.

4. **Risk evaluation** - by comparing the level of risk with the appetite for risk in the context already established. Based on this comparison, the need for treatment can be determined.

5. **Risk treatment** - can be viewed as a cyclical decision process which determine options/action plans for mitigating the risk and when implemented provides a control. Assessment of whether the remaining level of risk is tolerable will determine whether further action is required.
6. **Communication and consultation** - By engaging with the stakeholders to obtain and share information regarding to risk managements and risk treatments actions and to ensure basis for decisions is understood and if any particular actions are required. This step should take place during all stages of the process
7. **Monitoring and review** - This step should be as part of the process and involve a regular cycle of checking and test the risk descriptions and control activates against any changes in circumstances including Key Risk Indicators.

For more details refer to the Risk Management Process document, which includes relevant tools and guides.

Risk tolerance

While risk appetite is about the amount and type of risk that an organisation is willing to pursue or retain, risk tolerance is about what an organisation can actually deal with after controls. Risk tolerance is a management decision on whether the current level of risk is acceptable or not (decision to 'tolerate' the risk).

Risk tolerance is reflected in the risk consequence criteria that describe increasing levels of impact. The higher the impact the less likely the risk will be tolerated. In addition, risk tolerance can be reflected in the acceptability/escalation chart that determines the points where management intervention is required.

Therefore, risk tolerance reflects the application of risk appetite to specific risks or objectives. It is applied at the risk level, not at the same broad organisational level as risk appetite. There will be some occasions where an organisation can bear more risk (tolerance) than it is thought prudent to pursue (appetite).

2.3.1.3 First line risk reporting

- **Operational risks -** Within each division and region of the DET Central Office, risks to the achievement of their business plan objectives are recorded into a risk register. These should be regularly reviewed by the management teams. As a minimum, the risk co-ordinator within each division and region twice a year reports the reviewed risk data to the RDB.
- **Key operational risks -** As a result of the Group executive management team discussion, key operational risks are identified. These key operational risks are discussed by Executive Board. The key operational risks are highlighted for various reasons. It may be that they are the highest rated risks. They may be impacting across multiple divisions requiring a large number of resources to manage. They may be risks that are highly visible in the public domain or they may be risks that the Group feels needs the knowledge and support of the Executive Board to identify or confirm additional resource allocations.
- **Strategic risks -** Strategic risks impact across multiple Groups; they may even impact across other government departments and agencies. They are owned by members of the Executive Board. Each quarter, discussions are held with the Executive Board to conduct an in-depth analysis of selected strategic risks and to ratify the DET risk profile.
- **Project risks** should be monitored, reviewed and reported as required by the relevant project cycle. Reporting and escalation of risks should be considered in line with project governance arrangements, but should be reported to a Project Control Board or equivalent on a quarterly basis as a minimum. Throughout the project lifecycle, risk forums (e.g. workshops, discussion groups and/or stakeholder interviews) should be conducted on a regular basis to identify the key matters which could cause the project to deviate from its objectives.

Schools should regularly report to school council progress made on the implementation of the SSP and the AIP. These updates to council should include an outline of the key risks encountered in achieving the goals and objectives articulated in these plans.

2.3.2 Operation/implementation in the second line

The oversight and support functions provide supervision and guidance for the risk practices for the first line.

The strategic planning team provides the tools, framework and timings to enable the first line to effectively develop and manage their operational and strategic plans. Further details can be found here (Planning @ DET).

2.3.2.2 Second line risk management

The RDB and other teams provide advice and, where appropriate, critical review on operational risk management across the Department. They provide tools, guides and training to assist the first line to manage their risks.

Further information and guidance on the activities and services of the support functions can be found on the intranet at the following locations.
Risk and Decision Branch
Finance
Procurement
Information Technology
Information & Records Management
Human Resources
Fraud Management
Wellbeing and Safety
Insurance
Legal
Communications

Financial risk management

Included in the second line activities for the Finance Division, the Department is required to have a financial risk management policy and internal control system in place which addresses the risks associated with financial management. This is in accordance with the Government's Financial Management Compliance Framework, which incorporates the *Financial Management Act 1994*, The Department's Financial Risk Management Policy utilises the process identified in this Framework as its basis.

Business Continuity Management

Services delivered by the Department are essential to the Victorian community. A failure to deliver its services including its critical functions would have significant consequences. Business Continuity Management (BCM) is a program that aids the Department to prepare for "disruptive events" which may prevent the Department from continuing to deliver its services including its critical functions. Providing business continuity in the face of a disruptive event is important. BCM is an essential component of the Department's Risk Management Framework and commitment from all stakeholders is required to develop and implement sound BCM and build organisational resilience. Information on BCM is available through the Business Continuity Management page.

2.3.2.3 Second line risk reporting

The RDB generates various and regular reports to meet the decision making needs for senior management.

- The RDB facilitates, and provides quality assurance, for the first line risk review processes. This includes collation, and analysis, of operational risk information from groups, divisions and regions.
- An **analysis of DET's strategic and operational risk profiles** is carried out twice (at a minimum) each year for review at Executive Board. The analysis is undertaken in order to assess risk information, provide summarised information on key risk themes, define significant risk exposures to be considered at strategic level, evaluate key controls and risk treatments, review changes in risk exposure over time and identify potential improvements.

- **Portfolio Audit and Risk Committee (PARC)** - Upon completion of both the operational and strategic risk review processes twice yearly reports are prepared for PARC:
  - the total number of risks and their ratings
  - a risk profile heat map
  - a comment on trends and themes
  - statistical data analysis.

Other second line functions provide regular reporting to the management teams in the Department and can include financial, human resource, procurement and wellbeing/safety reports.

2.3.3 Operation/implementation in the third line

Risk assurance activities are designed to ensure risks are being appropriately managed, provide validation of the effectiveness of controls and stimulate a continuous improvement cycle.

2.3.3.1 Internal audits

Audits are delivered using a co-sourced arrangement. PARC is required to approve the four-year rolling Portfolio Internal Audit Plan including the annual audit plan, oversee its delivery and consider audit reports. The Portfolio Internal Audit Plan provides for:

- compliance audits – determining adherence to relevant legislation, policies or procedures
- operational and IT audits – assessing the reliability, integrity and adequacy of financial, operational and IT systems, processes and procedures within a program or operational area
- performance audits – examining the efficiency, effectiveness, economy of a policy, program, project or function within the Department.

Audit activities are overseen by PARC with PARC meeting minutes approved by the Secretary.

Management is responsible for improving internal controls in response to audit findings. Audit findings (except for VAGO performance audit findings) are assigned audit ratings.

The Assurance Branch performs a quarterly follow-up to provide assurance regarding management's implementation of audit actions.

2.3.3.2 Government school audits

Victorian government schools are included in the Department's risk-based Portfolio Internal Audit Plan. In addition, a number of schools are selected annually for audit/review of financial management controls, balances and transactions for the purposes of departmental financial year-end audit, i.e. consolidation of schools' accounts with DET's accounts. Auditors are required to (not an exhaustive list):

- examine the financial activities of the school including trading operations
- examine the school's financial risks and internal controls
- examine school council governance with respect to financial risks and internal controls and budgetary management.

2.3.4 Calendar of risk management activities

Risk management is an ongoing process throughout the year. Recommended timing for specific activities within the risk management framework are outlined in Table 1.

Table 1 – Calendar of risk management activities

	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun
Strategic Risk												
DET Strategic Risks (Executive Board)	🟪			🟪			🟪			🟪		
Group Strategic Risk Review											🟦	🟦

	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun
Operational Risk												
Key Operational Risks (Executive Board)				🟫						🟫		
Group Risk review			🟦						🟦			
Division Risk Review*		🟨	🟨					🟨	🟨			
Project Risk												
Key Program/Project Risks (Executive Board)	🟪	🟪	🟪	🟪	🟪	🟪	🟪	🟪	🟪	🟪	🟪	🟪
Project/Program Risk Review*	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧
Executive/Regional Director Sub-Attestation												🟦
Secretary Attestation	🟫											
Risk Management Framework Review										🟦	🟦	🟦
PARC Review		🟩		🟩		🟩			🟩		🟩	🟩
Risk Training	🟩	🟩	🟩	🟩	🟩			🟩	🟩	🟩	🟩	🟩

* It is recommended that the divisions and projects review and discuss their risk information at regular management and project meetings

2.4. Monitoring and review of the Framework

The Framework requires regular monitoring and review to assess the effectiveness of its design and implementation. This is provided by internal and external assessments and continual review by the RDB.

2.4.1 RDB review and monitoring

The RDB will continually review the risk management framework and the effectiveness of its implementation. The RDB utilises the inputs from other internal and external reviews.

To validate any improvements, the RDB will:

- conduct risk maturity assessments
- undertake risk culture surveys
- participate in peer reviews and discussions of latest developments in the field of risk management
- regularly meet to review and identify opportunities for improvements
- ensure the Framework is aligned to the latest Risk Management Standards and Regulations.

The RDB also generates reports on the Department’s risk profile, the maturity of risk management and the implementation of the Framework to the Executive Board and the PARC semi-annually.

Outputs of these review practices feed into the Risk Management Strategy.

2.4.2 Internal reviews

2.4.2.1 Audit outputs

In line with the Portfolio Internal Audit Plan, the internal audit team will undertake audits of part or all of the implementation of the Risk Management Framework.

2.4.2.2 Attestation

In support of the *Public Administration Act 2004*, and as part of the Standing Directions of the Minister for Finance under *the Financial Management Act 1994* (August 2007), the Secretary is required to provide an attestation (a confirmation of correctness or truth) in the Department’s annual report stating that the Department understands, manages and controls key risk exposures consistent with the AS/NZS ISO 31000:2009. A responsible body or audit committee must also verify this view. In the Department, to complete this activity:

- **risk management sub-attestation statements** are completed by Deputy Secretaries, Executive Directors and Regional Directors annually. These sub-attestations support the Secretary's risk attestation statement
- the **Risk Attestation Statement** is verified by the PARC before it is signed by the Secretary and published in the Department's Annual Report.

2.4.2.3 Customer satisfaction surveys

RDB conducts ongoing customer satisfaction surveys to assess client advocacy. It also:

- translates perceptions into quantitative data that can be used to target areas for improvement
- provides a base line measurement to build upon.

2.4.3 External reviews

2.4.3.1 Victorian Managed Insurance Authority review

The Victorian Managed Insurance Authority (VMIA) is a statutory body, whose operations are governed by the *VMIA Act 1996*. Under the Act, the VMIA's functions include assisting agencies to establish programs for the identification, quantification and management of risks and to monitor risk management.

The VMIA will be requested to undertake periodic systematic and independent reviews of the Risk Management Framework in order to determine the maturity and effectiveness of risk management within the Department at intervals not exceeding three years.

2.4.3.2 Risk culture surveys

A Culture Survey assesses whether or not DET has a culture which embraces risk management. The survey will provide us with insights into the attitudes within our organisation to the management of risk and monitors changes over time in organisational attitudes to the management of risk.

2.4.3.3 Victorian Auditor-General's Office review

VAGO may audit any aspect of risk management within the Department. These audits are a key source of continual improvement to the Department's risk management practices.

2.5. Continual improvement

To support continual improvement; the RDB will:

- conduct the risk management culture survey
- provide ongoing training and development for RDB stuff
- regularly assess the risk management process and identify opportunities for improvements
- align the Framework with the Risk Standards and Regulations
- take outputs from the monitoring and review processes to review and update the Risk Management Strategy.

2.5.1 Risk management strategy

The Risk Management Strategy supports the Department's Risk Management Framework with the intention of improving and enhancing existing risk management practices throughout the organisation to help the Department achieve its objectives. The strategy will be updated and approved by Executive Board annually and is found here.

While the RDB takes the lead in the iterative process of continuous improvement, all executive officers, principals, and managers are responsible for promoting the application of risk management including provision of appropriate training in risk management and delivering ongoing improvements to risk management processes and guidelines.

The RDB continues to develop new tools to assist and improve the management of risk including in response to events or changing circumstances.

Appendix A Risk Terminology/Glossary

Common risk terminology/language

Standardising risk management terminology promotes knowledge sharing and transfer so that an individual who gains their initial understanding of risk management in one domain will be able to utilise those skills in another domain (e.g. later in their career when they have transitioned from teacher to assistant principal and are working to develop their school's strategic plan).

In part the terminology of the Department is detailed within this Framework and the glossary below. It is also ascribed by the tools and techniques which form part of the Framework and to some extent it will grow as the Department's risk culture continues to grow.

Many of the definitions below are derived from Standards Australia and, where appropriate, modified for the Department.

Term	Definition
ALARP	As Low As Reasonably Practical
Business Continuity Management (BCM)	The process by which 'business as usual' or 'continuity of operation/services' is addressed to ensure critical business activities can be continued and resources restored, following an operational disruption.
Consequence	Outcome of an event affecting objectives (can be positive or negative).
Control	Measure that is modifying risk in business as usual state.
Current risk	Risk present in the business as usual state i.e. with existing controls
Event	Occurrence or change of a particular set of circumstances
Exposure	Extent to which we may be subject to an event. It can also relate to proximity to an event in terms of space or time i.e. proximity to bush fire danger area or to fire season.
FMCF	Financial Management Control Framework
Likelihood	Chance of something happening
PARC	Portfolio Audit and Risk Committee
Resilience	Adaptive capacity of an organisation in a complex and changing environment
Risk appetite	Amount of risk the Department is prepared to seek or accept in pursuit of objectives
Risk matrix	Standard tool for rating risk by defining ranges for consequence and likelihood
Risk owner	Person with the accountability and authority to manage a risk
Risk tolerance	The limits of risk-taking, beyond which the Department will not go, even to pursue objectives
Source	Element that alone or in combination has the intrinsic potential to give rise to risk
SPAG	School Policy and Advisory Guide
Target risk	Risk remaining after (risk) treatment
Treatment	Process/action to modify risk
The Policy	The Risk Management Policy which provides guidance on the principles, mandatory requirements and accountabilities
Treatment	Process to modify risk
VAGO	Victorian Auditor-General's Office
VMIA	Victorian Managed Insurance Authority