Office of the Information Commissioner
Queensland

RISK MANAGEMENT PLAN

1. Introduction

Risk Management is a logical and systematic process that can be used when making decisions to improve the effectiveness and efficiency of organisational performance. Although most risks cannot be eliminated altogether, the management of risk involves identifying and being prepared for the occurrence of adverse events and taking action to avoid or reduce unwanted exposures of the organisation to an acceptable level.

Risk management encourages the Office to manage proactively rather than reactively. Therefore, it also means identifying and taking opportunities to improve organisational performance as much as it means taking action to avoid or reduce the chances of something going wrong.

An integrated risk management system involves a systematic and rigorous approach to what people do on a daily basis. However, it is not complex and does not require specialised skills.
Purpose

2. Purpose

The purpose of this plan is to facilitate the development of a risk management culture within the Office and to assist all staff in implementing sound risk management practices that eliminate or minimise potential losses and add value to the business operations of the Office.

In applying risk management principles it is expected that officers at all levels will:

- Seek to reduce vulnerability to both internal and external events and influences that can impede achieving the goals of the Office
- Seek to capitalise on opportunities to enhance service delivery and create value
- Contribute to effective corporate governance

3. Risk Management in the Office

The Office risk management framework is designed to encourage an integrated approach to managing all risks in the Office that impact on the achievement of our strategic and business objectives. It is built around having a common language and common approach to help us identify which risks are really important, what we do, and how we allocate Office resources to deal with them.

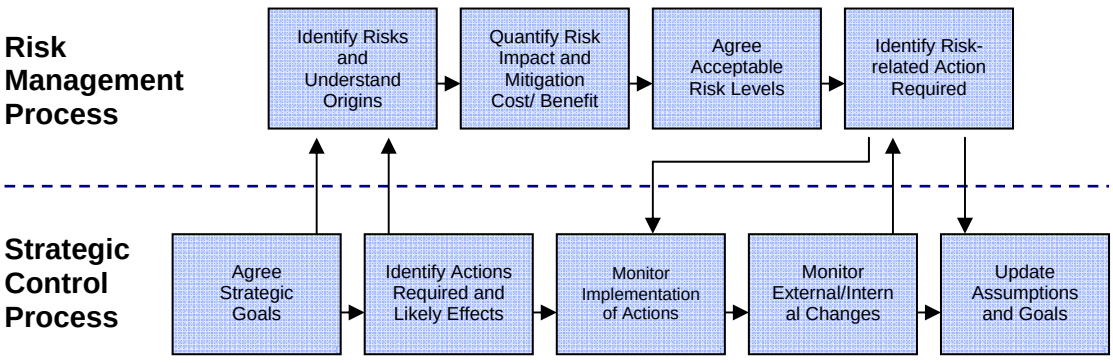
Applying risk management means adopting a systematic approach to how we view our environment identify issues that may impact on the achievement of our objectives, develop strategies to address significant risks, and take advantages of opportunities. The benefits and potential impact of risk management in the Office are outlined below.

What are the benefits?	What impacts are likely to result?
Supports the process of business and strategic change including development of objectives and performance measures	Better achievement of desired programme outcomes
Focus of effort on key risks to achievement of objectives	
Customer, taxpayer, public, business focus for decision making	Improved service delivery
Resources released from over-controlled lower risk areas	Better value services
Platform for risk taking and innovation	More opportunities taken to deliver services in innovative ways
Identification of opportunities	
Better contingency planning	Better management of the unexpected and continuity of essential service delivery
Reduced uncertainty and scope for surprises	

Risk management is not new. Nor is it an unstructured, one off exercise. In the framework of Office objectives, risk management is linked to the strategic planning and business planning process. With strong accountability and an understanding of the environment in which we operate, the implementation of a robust risk management framework will facilitate a forward thinking approach to how the Office does business.

4. Corporate Governance

Corporate Governance is the way in which an organisation is controlled and governed in order to achieve its objectives. This controlled environment makes an organisation reliable in achieving its objectives within an acceptable degree of risk. The Office is committed to establishing an organisational philosophy and culture that ensures risk management is an integral part of all activities. When implementing risk management, it is more efficient to fully integrate the management of risks into existing management practices.



Integrating the Office risk management process into normal practices should not become an additional overhead that employees of the Office have to bear. There is considerable scope to enhance the Office corporate governance practices with little additional effort by building on the linkages between risks, returns and resources. Formal integration of these and other governance practices, such as corporate planning, quality assurance, regular reporting and internal audit, within a coordinated management cycle will achieve this.

5. When should risks be managed?

Risk should be managed continuously. All decisions involve management of risk in some kind or another. Whether they be decisions which are taken in every day operations (such as deciding work priorities, making budgetary or staffing decisions) or decisions about major policies, strategies, or projects which involve the commitment of large amounts of money and resources, the effective application of risk management is essential.

It is desirable to develop a mindset of a conscious approach to managing the risks inherent in every decision. Many decisions have to be made quickly and are often based on intuition, but it is nevertheless important to think about the risks involved.

The step-by-step process for managing risk, contained in this guide, should be applied to decision making at all levels throughout the Office of the Information Commissioner.

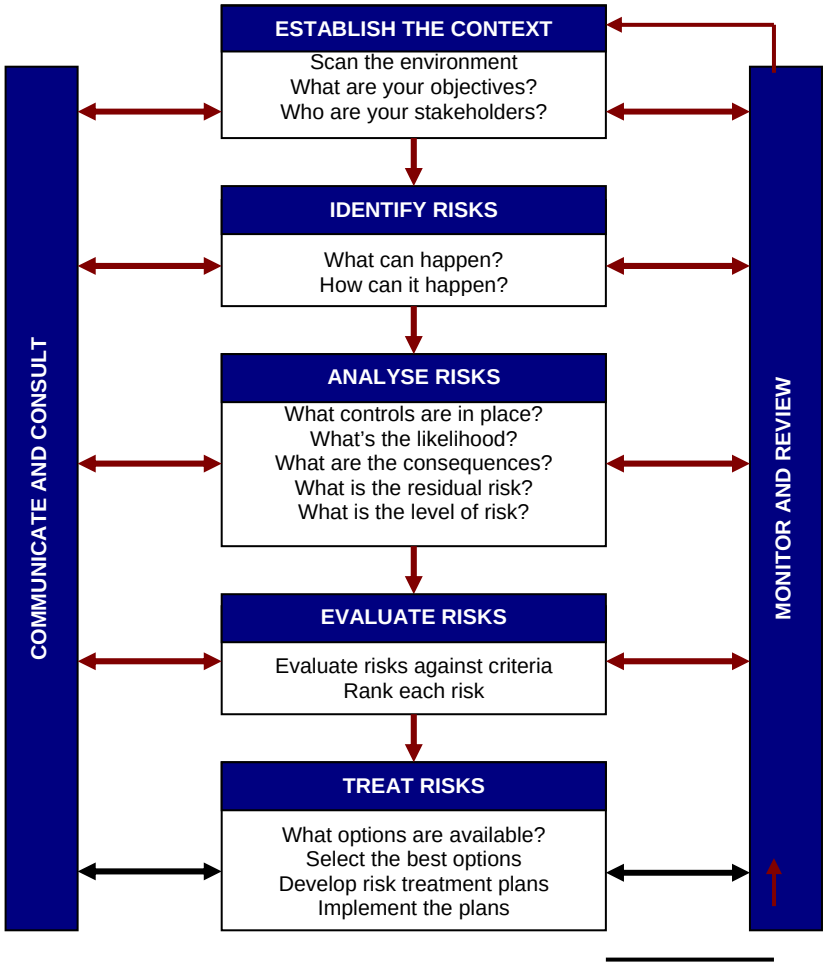
6. Risk Management Approach

The Office's risk management policy aims to ensure:

- A common and consistent approach to the management of risks is adopted across the Office, and
- All significant risks to the Office are identified, evaluated, managed, and reported to the Information Commissioner.

7. Risk Management Process

In line with these objectives, the following approach will be adopted:



8. Identifying Risks

8.1 Purpose

This step seeks to identify the risks that could affect achieving the objectives of the Office. It is fundamental to the success of the risk management process that the widest range of risks are identified at this stage. Risks not identified cannot be assessed and treated as part of this process, and as a result, may become significant exposures at a future time.

8.2 Actions

Risk identification involves examining all sources of risk and the perception of all stakeholders.

Example sources of risk in the Office may include, but are not limited to:

- Management activities
- Human resources and behaviour
- Financial and marketing activities
- Reporting and accountability requirements
- Technology and technical issues
- Conduct of external reviews
- Security
- Processes and procedures
- Interfaces and communication
- Individual activities
- Commercial and legal relationships
- Organisational culture
- Natural events

Valid information is important in identifying risks and in understanding the likelihood and consequences of the risk. Although it is not always possible to have the best, or all information, it should be as relevant, comprehensive, accurate, and timely as resources will permit. Existing information sources need to be accessed and where necessary, new data sources developed.

Possible methods for identifying risks may include:

- Surveys
- Questionnaires or checklists
- On-site inspections and audits
- Personal experience or past organisational experience
- Examination of local or overseas experience
- History and failure analysis
- Scenario analysis
- Flow Charting

8.3 Key Questions for Identifying Risk

Why does this situation represent a risk?
Why would it impact on achieving objectives?
How can it happen?
What is the potential cost in time, money and resources?
What is the nature of the risk?
What controls presently exist to mitigate the risk?
Who might be involved in the occurrence of the risk?
Is there a need to investigate and research specific risks or seek further information?

8.4 Outcomes

The output of this step is a comprehensive list of possible risks to the successful achievement of the organisation's objectives.

Identified risks are documented in the Risk Management Matrix (Attachment A).

9. Treating Risks

9.1 Purpose

This step is to determine what will be done with risks determined as being unacceptable to the organisation. Potential risk treatment options are evaluated in terms of feasibility, costs, and benefits. The option chosen should be the most appropriate and practicable, with the objective of reducing the level of risk to an acceptable level or as low as reasonably practicable.

9.2 Actions

Risk treatment involves two steps:

- determining risk treatment strategies, and
- developing and implementing the Risk Treatment Plan.

9.2 Risk Treatment Strategies

Risk treatment options include:

- Reducing the Likelihood – Limiting the chance that the risk will occur by undertaking specific actions, e.g. audit and compliance programmes, inspection and process controls, preventative management, and structured training.
- Reducing the Consequence – Minimising the impact of the risk, should it occur, by developing consequence reduction strategies, e.g. contingency planning, crisis management, public relations, and business continuity plans.
  (The development and ongoing maintenance of business continuity plans for critical organisational functions and services are an essential treatment strategy to ensure that service to the public is maintained or quickly recovered following a disaster).
- Transferring the Risk – Shifting responsibility for the risk to another party, who ultimately bears some of the consequences if the risk occurs, e.g. insurance and contractual arrangements

The process of selecting and developing the most effective treatment option for each identified risk involves:

- assessing the feasibility and potential benefits and costs of each option
- selecting the best option and
- determining how the treatment will be implemented

The following table provides an indication of the level of attention and responsibility for the treatment of various levels of risk.

LEVEL OF RISK	DEFINITION
Low Risk	Manage by routine procedures in the Office.
Medium Risk	Manage by specific monitoring or response procedures in the Office.
High Risk	Senior management attention needed and management responsibility specified. Treatment strategies determined and implemented under the accountability of senior management.
Extreme Risk	Immediate action required Senior management attention needed and responsibility specified. Treatment strategies determined and implemented under the accountability of senior management.

Any existing controls or plans in place prior to the commencement of the risk management process should also be taken into consideration when developing risk treatments strategies. These controls or plans may be augmented by selected treatment strategies.
A risk that cannot be reduced to an acceptable level, but is essential to the achievement of a departmental objective/s, should be reduced to as low as reasonably practicable. This may involve developing and invoking specific treatment strategies, and in addition, maintaining a higher level of monitoring, e.g. weekly monitoring of the risk rather than monthly monitoring.

9.3 Risk Treatment Plan

Once determined, a risk treatment strategy, and the process for its implementation, should be documented in the Risk Treatment Plan (Attachment A).

The Risk Treatment Plan should be included as a part of existing management plans, coordinated and integrated wherever possible with established management processes and procedures, and controlled and managed like any other activity. This may require risk treatments to be integrated with existing procedures for budgeting, health and safety, human resources and other activities as appropriate.

9.4 Key Questions for Treating Risks

What processes and controls exist, or are needed, to minimise the level of risk?
What is the feasibility and cost effectiveness of each treatment options?
What resources are needed (people, funding, technical)?
Do the risk treatments comply with legal requirements, government and organisational policies, including those concerning access, equity, ethics and accountability?
Who has the responsibility for implementing the plan for managing risks?

10. Monitoring and Reviewing Risks

10.1 Purpose

This step is to link risk management to other organisational management processes (e.g. business planning) and to facilitate better risk management and continuous improvement.

Regular monitoring and review of risks to the organisation ensures new risks are detected and managed, any changes to existing risks are detected and managed, and action plans are implemented effectively.

10.2 Actions

Monitoring and reviewing the risk management process for the organisation involves:

- Determining whether each risk previously identified is still relevant to the organisational area
- Reviewing the assessments given to likelihood and consequences for each risk
- Reviewing the risk rating
- Reviewing the adequacy of existing systems and controls to manage risk and
- Reviewing the treatment strategies that previously have been considered and are currently being implemented

Monitoring and review of risk should be synchronised with normal business control processes, that is, at the occurrence of business performance benchmarking (e.g. quarterly). This process allows for the effective revision of previously identified risks, and associated treatment strategies being implemented for their mitigation, and provides the opportunity to determine and undertake the risk assessment process for any new risks which should be included.

The organisation's risk register is the main tool for monitoring risks.

10.3 Key Questions for Monitoring and Review

Are the risk treatments effective in minimising the risks?

Are the risk treatments comparatively efficient/cost effective in minimising risks?
Are the management and accounting controls adequate?
Do the risk treatments comply with the legal requirements, government and organisational policies, including access, equity, ethics and accountability?
How can improvements be made?

11. Reporting Timelines

Risk reporting to the Information Commissioner occurs twice a year:

- Following the completion of the External Audit of the financial year and
- In conjunction with the finalisation of the strategic plan.

This report should include:

- Risk category – the category of risk under which the identified risk falls,
- Description of the risk – what the risk is, cause and effect,
- Last half year level of risk – the likelihood and consequence ratings of the risk determined during the business planning process (risk may be newly identified or ongoing from previous cycle),
- Action being taken – a description of the risk treatment options being implemented to manage the risk,
- Current level of risk – the likelihood and consequence ratings of the risk determined at the half year (six months) reporting date. These ratings should reflect the affect of the treatment strategies being implemented to manage the risk.

ATTACHMENT A

EMERGENCY/DISASTER/RISK IDENTIFICATION AND TREATMENT PLAN

Risk Category	Details of Risk, Emergency or Disaster	Risk Level	Treatment	Actioned By	When
Reputation	Inappropriate staff performance or conduct	Low	All staff receive training and are aware and compliant with policies and legislation governing their actions and decisions regarding their work undertaken as employees of the Office. Code of Conduct training	• Staff Meeting • Personal Performance Plan	Code of Conduct training held annually
	Office culture	Low	The Office culture is to openly discuss potential and identified risks and determine the appropriate resolution. Code of Conduct training	• Staff Meetings	Code of Conduct training held annually
	Confidentiality	Low	All staff and external suppliers have signed confidentiality agreements in place prior to work commencing with the Office. Code of Conduct training	• Senior Corporate and Executive Services Officer	As required
	Independence	Low	The Information Commissioner is independent of executive government, reporting to a Parliamentary Committee and cannot be directed as to the operation of functions performed by the Office.	• Information Commissioner	Ongoing
	Independence	Low	The Office does not use any Queensland Government logo in any communications, publications or on the website.	• Communications Officer • Office Manager	Quarterly Check
	Information accuracy	Low	Review publications for accuracy	• Training and Stakeholder Relations Manager	Quarterly Check
Information Security	Information security – External Review Unit	Low	All access application 'matter in issue' is stored in the designated secure room with dedicated security access. This secure room is located within the Office premises which have a range of further security protections.	• External Review staff • Registry staff	On going
	Information security – Privacy Unit	Low	All privacy complaint files are stored in the designated secure room with dedicated security access. This secure room is located within the Office premises which have a range of further security protections.	• Privacy staff	On going
	Information security – Assistance and Monitoring Unit	Low	All agency access application files and material associated with compliance assessment evaluation by the Performance Monitoring and Reporting Team are stored in the designated access room with dedicated security access. This secure room is located within the Office premises which have a range of further security protections.	• Performance Monitoring and Reporting staff	On going

	Information	Low	Emails, Electronic data and mail is registered and handled in accordance with set procedures.	• Registry staff	Daily
	Server failure	Low	Refer to the Operating Level Agreement between the Office and the Queensland Parliamentary Service for process and procedure to interruption of service.	• MCES	On occurrence
Staff Security and Safety	Staff security	Low	The Office is a secure area except for the reception area. Meetings involving non-Office staff must be held in the conference room or mediation rooms which have two separate lockable entry points and are fitted with duress alarms. The Office electronic security system is connected to the State Government Protective Security Service and on-site security.	• All staff	On occurrence
	Dealing with volatile people	Low	Staff receive training, mentoring and debriefing in relation to interacting with volatile people. An Employee Assistance Scheme (EAS) support service is available. Code of Conduct training Security training at induction	• Senior Corporate and Executive Services Officer • Executive Leadership Team • MCES • Office Manager	On going
	Natural disaster	Low	Treatment strategy to be determined by Information Commissioner and communicated to key stakeholders in accordance with Emergency Communication Plan.	• Information Commissioner • Executive Leadership Team • MCES	On occurrence
	Building emergency	Low	Refer Office Emergency Response Plan Education at staff meetings and induction	• Floor Wardens • MCES • First Aid Officers	On occurrence