Office of the Information Commissioner
Queensland

Risk Management Framework

October 2018

Contents

1. Introduction and purpose

1.1. Introduction

Risk can be defined as *the effect of uncertainty on objectives*[1].

Risk management is the process for managing, rather than avoiding risk. A proactive approach to risk management allows effective engagement with risk, both to mitigate against threats and to seize opportunities.

Risk management is used to make decisions to improve the effectiveness and efficiency of the Office of the Information Commissioner (OIC).

An integrated risk management system involves a systematic and rigorous consideration of what people do and how they do it, on a daily basis. However, it is not complex and does not require specialised skills.

1.2. Purpose

The purpose of this framework is to set out the OIC's approach to risk management – our governance, systems, process and culture that support us to engage effectively with risk.

The framework is supported at an operational level through operational planning and procedures relevant to particular activities and / or projects.

2. Risk management framework

2.1. Governance and assurance

Corporate governance is the way in which an organisation is controlled and governed in order to achieve its objectives. The OIC's governance and assurance strategies for risk management reflect the functions and size of our agency.

The OIC Governance Committee provides oversight of the OIC's risk management framework and operational management of risks.

The Committee is supported by the OIC Risk Advisory Group, whose role is to provide advice and recommendations to support OIC's risk management approach. **Appendix one** sets out the Terms of Reference for the OIC Risk Advisory Group.

Periodic reviews of the OIC's risk management framework and its implementation may also be undertaken by internal audit.

2.2. Systems

This part of the framework sets out the systems that support the OIC's management of risk. It recognises that the effective management of risk requires a multi-faceted approach, with engagement from an educated and aware workforce.

[1] AS/NZ ISO 31000:2009 Risk management – principles and guidelines

(a) Culture and awareness

The OIC is committed to establishing a culture that ensures risk management practices are an integral part of our activities; risk awareness and engagement is recognised as part of our day-to-day business not as a separate one-off activity.

The OIC will support a risk aware (not risk averse) culture through:

- developing staff awareness of roles and responsibilities in the identification and management of risks
- promoting the benefits of effective risk management
- responding appropriately to staff engagement with risk, aligned with our risk appetite statement.

(b) Risk appetite statement

The OIC's risk appetite statement provides guidelines on our engagement with different categories of risk. It reflects our willingness to assume, or be exposed to, certain levels of risk in order to achieve our objectives.

The OIC's risk appetite statement is set out in **Appendix two**

(c) Tools

To assist in the identification, analysis and monitoring of risks, the OIC utilises a range of tools:

- risk matrices (**Appendix three**)
- a risk register. The process for reviewing and updating the register is set out below.

2.3. Processes

The risk management process is a continuing cycle, represented by the below figure.

The Risk Advisory Group acts on behalf of OIC's business units to identify and assess risks associated with our business, to assess treatments and determine residual risk.

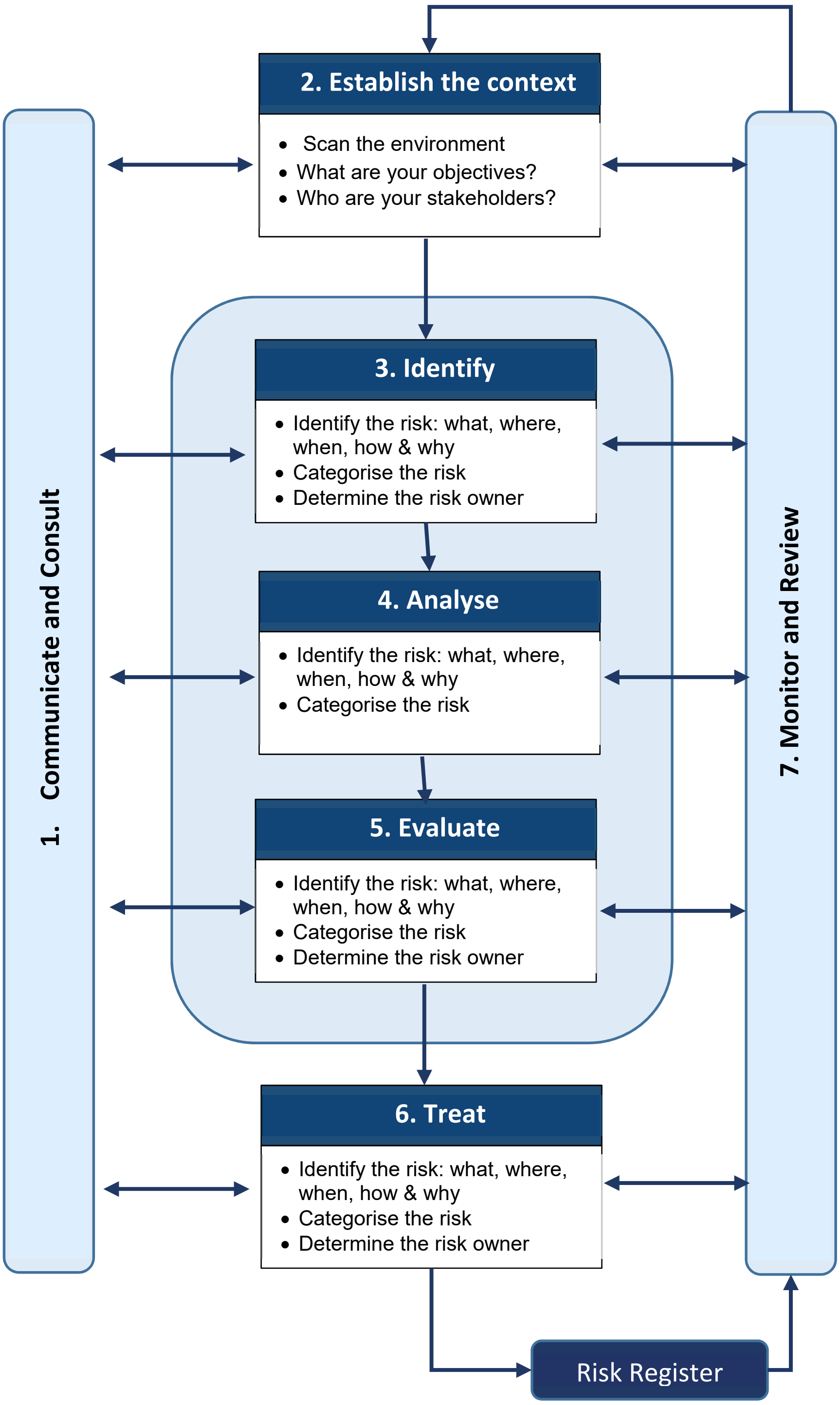
- **Appendix four** sets out a range of questions that can assist in identifying risks
- **Appendix five** sets out strategies to treat risks.

Every quarter the Governance Committee will review risks assessed as high or extreme, or where the current risk level exceeds the target risk level, along with progress towards the implementation of approved risk treatments. Annual reviews of risks will be undertaken by the Risk Advisory Group.

Ad hoc reviews will occur as required, for example due to changes in context or as a result of incidents occurring.

All staff are responsible for ongoing monitoring of risks and identifying changes, incidents or treatments.

Questions to assist in monitoring risk are set out in **Appendix six**.



1. Communicate and Consult

2. Establish the context

- Scan the environment
- What are your objectives?
- Who are your stakeholders?

3. Identify

- Identify the risk: what, where, when, how & why
- Categorise the risk
- Determine the risk owner

4. Analyse

- Identify the risk: what, where, when, how & why
- Categorise the risk

5. Evaluate

- Identify the risk: what, where, when, how & why
- Categorise the risk
- Determine the risk owner

6. Treat

- Identify the risk: what, where, when, how & why
- Categorise the risk
- Determine the risk owner

7. Monitor and Review

Risk Register

Adapted from AS/NZS ISO 31000 risk management process

Appendix One: Risk Advisory Group Terms of Reference

Purpose

The OIC Risk Advisory Group is established to provide advice and recommendations to the OIC Executive Team to support OIC's risk management approach.

The OIC Risk Advisory Group is established in line with recommendations arising out of the OIC Internal Audit on Risk Management (May 2018).

Outcomes

1. To contribute to the OIC Risk Management Framework, the OIC Risk Advisory Group will:
    - identify risk categories
    - determine risk appetite for each risk category
    - assess risks, identify existing controls, recommend control and determine residual risk.
2. To support the Executive Team in the effective management of risk by contributing to regular reviews of the risks and controls, in accordance with the OIC Risk Management Framework.

Timeframe and meetings

The OIC Risk Advisory Group will deliver Outcome 1 no later than 14 September 2018 to enable consideration by the OIC Executive Team by 30 September 2018.

Meetings will occur fortnightly unless otherwise agreed by the members.

Membership

The OIC Risk Advisory Group is made up of representatives from across OIC:

- External Review – Kristen McGuire
- Audit and Evaluation – Sandra Heidrich
- Privacy – Danielle Barnes
- Corporate (Training and Stakeholder Relations) – Steven Haigh
- Corporate (Information and Assistance) – Kathryn Taylor
- Corporate (Business Services incl. Registry) – Stephanie Mitchell.
- Executive team representative – Vivienne Van Der Laak

Where a member is unable to attend a scheduled meeting, they will take reasonable steps to arrange a suitably briefed delegate.

Membership will be reviewed at least annually.

Audit recommendations

1. Audit recommends that a Risk Management Policy (Framework) be developed. The Policy would incorporate much of the information already contained in the Risk Management Plan but include additional information such as likelihood and consequence definitions and more agency specific information.
2. Audit recommends that a formal review of the agency's risks be undertaken with input from all staff but particularly from senior management. All risks identified should be evaluated in terms of consequence and likelihood and evaluated in accordance with the agency's framework. Such reviews should be done periodically and at least formally once a year.
3. A Risk Register should be created to document the agency's risks. In this respect Audit has provided management with a "pro-forma" register which could suit OIC's requirements.

Endorsed by OIC Executive Team on 3 July 2018

Appendix Two: Risk Appetite

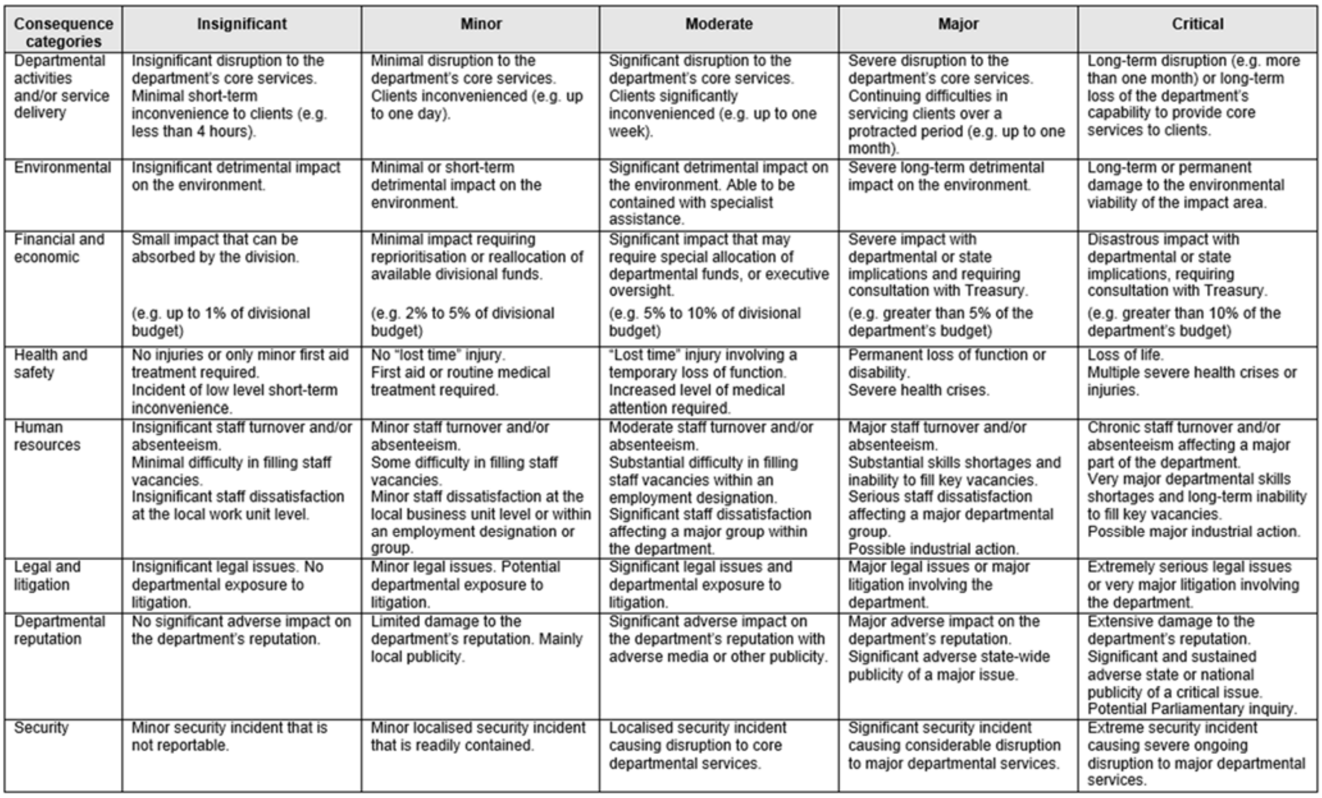
Category	Risk Appetite
Health, safety & well-being	We value the health, safety and well-being of our staff. We have a low appetite for risks to health, safety and well-being of our people, however we recognise that there are inherent risks associated with our role and functions. We will take reasonable steps to minimise such risks.
Fraud & corruption	The OIC is an independent statutory office that forms part of Queensland's integrity framework. We have a low appetite for risks associated with fraud and corruption. We will take all reasonable steps, commensurate with our size and function, to eliminate or mitigate such risks.
Information Management	The OIC handles a range of confidential, personnel or otherwise sensitive information. We have a low appetite for risks that compromise effective information management. We will take all reasonable steps, commensurate with our size and available resources, to eliminate or mitigate such risks.
ICT	The OIC recognises that an effective ICT environment is central to the effective discharge of our statutory obligations. We have low appetite for ICT risks that could compromise the security of our information holdings or the delivery of our services. We will take all reasonable steps, commensurate with our size and available resources, to eliminate or mitigate such risks.
Service delivery	We are committed to the delivery of our services in an effective, efficient and timely manner. We recognise the importance of innovation to our service delivery. We accept that trying new ways of working has inherent risks and will mitigate against these proportionate to each activity.

Appendix three: Risk Matrices

Likelihood

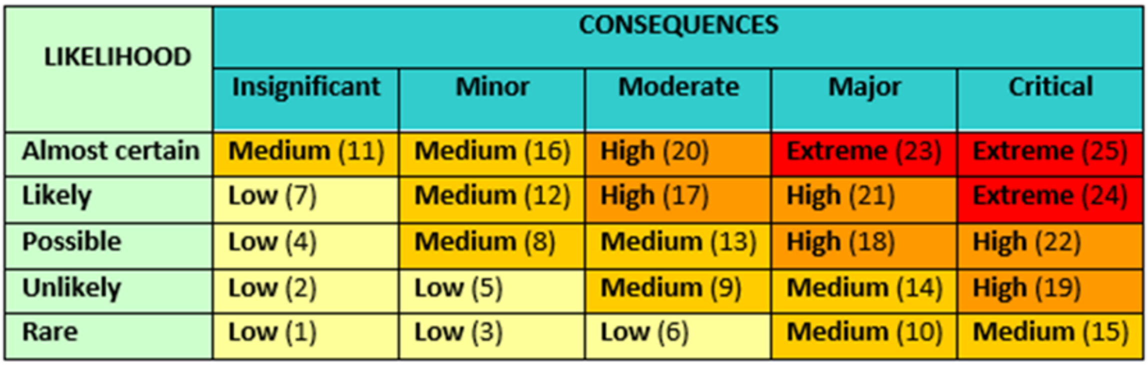
Likelihood	Qualitative description	Quantitative description
Almost Certain	The event is expected to occur in most circumstances	May occur once a month or more frequently
Likely	The event will probably occur in many circumstances	May occur once every year
Possible	Identified factors indicate the event could occur at some time	May occur once every 2 or 3 years
Unlikely	The event could occur at some time but is not expected	May occur once every 5 years
Rare	The event may occur only in exceptional circumstances	May occur once every 10 years

Consequence



Consequence categories	Insignificant	Minor	Moderate	Major	Critical
Departmental activities and/or service delivery	Insignificant disruption to the department's core services. Minimal short-term inconvenience to clients (e.g. less than 4 hours).	Minimal disruption to the department's core services. Clients inconvenienced (e.g. up to one day).	Significant disruption to the department's core services. Clients significantly inconvenienced (e.g. up to one week).	Severe disruption to the department's core services. Continuing difficulties in servicing clients over a protracted period (e.g. up to one month).	Long-term disruption (e.g. more than one month) or long-term loss of the department's capability to provide core services to clients.
Environmental	Insignificant detrimental impact on the environment.	Minimal or short-term detrimental impact on the environment.	Significant detrimental impact on the environment. Able to be contained with specialist assistance.	Severe long-term detrimental impact on the environment.	Long-term or permanent damage to the environmental viability of the impact area.
Financial and economic	Small impact that can be absorbed by the division. (e.g. up to 1% of divisional budget)	Minimal impact requiring reprioritisation or reallocation of available divisional funds. (e.g. 2% to 5% of divisional budget)	Significant impact that may require special allocation of departmental funds, or executive oversight. (e.g. 5% to 10% of divisional budget)	Severe impact with departmental or state implications and requiring consultation with Treasury. (e.g. greater than 5% of the department's budget)	Disastrous impact with departmental or state implications, requiring consultation with Treasury. (e.g. greater than 10% of the department's budget)
Health and safety	No injuries or only minor first aid treatment required. Incident of low level short-term inconvenience.	No "lost time" injury. First aid or routine medical treatment required.	"Lost time" injury involving a temporary loss of function. Increased level of medical attention required.	Permanent loss of function or disability. Severe health crises.	Loss of life. Multiple severe health crises or injuries.
Human resources	Insignificant staff turnover and/or absenteeism. Minimal difficulty in filling staff vacancies. Insignificant staff dissatisfaction at the local work unit level.	Minor staff turnover and/or absenteeism. Some difficulty in filling staff vacancies. Minor staff dissatisfaction at the local business unit level or within an employment designation or group.	Moderate staff turnover and/or absenteeism. Substantial difficulty in filling staff vacancies within an employment designation. Significant staff dissatisfaction affecting a major group within the department.	Major staff turnover and/or absenteeism. Substantial skills shortages and inability to fill key vacancies. Serious staff dissatisfaction affecting a major departmental group. Possible industrial action.	Chronic staff turnover and/or absenteeism affecting a major part of the department. Very major departmental skills shortages and long-term inability to fill key vacancies. Possible major industrial action.
Legal and litigation	Insignificant legal issues. No departmental exposure to litigation.	Minor legal issues. Potential departmental exposure to litigation.	Significant legal issues and departmental exposure to litigation.	Major legal issues or major litigation involving the department.	Extremely serious legal issues or very major litigation involving the department.
Departmental reputation	No significant adverse impact on the department's reputation.	Limited damage to the department's reputation. Mainly local publicity.	Significant adverse impact on the department's reputation with adverse media or other publicity.	Major adverse impact on the department's reputation. Significant adverse state-wide publicity of a major issue.	Extensive damage to the department's reputation. Significant and sustained adverse state or national publicity of a critical issue. Potential Parliamentary inquiry.
Security	Minor security incident that is not reportable.	Minor localised security incident that is readily contained.	Localised security incident causing disruption to core departmental services.	Significant security incident causing considerable disruption to major departmental services.	Extreme security incident causing severe ongoing disruption to major departmental services.

Risk Level



LIKELIHOOD	CONSEQUENCES				
	Insignificant	Minor	Moderate	Major	Critical
Almost certain	Medium (11)	Medium (16)	High (20)	Extreme (23)	Extreme (25)
Likely	Low (7)	Medium (12)	High (17)	High (21)	Extreme (24)
Possible	Low (4)	Medium (8)	Medium (13)	High (18)	High (22)
Unlikely	Low (2)	Low (5)	Medium (9)	Medium (14)	High (19)
Rare	Low (1)	Low (3)	Low (6)	Medium (10)	Medium (15)

Appendix four: Identifying risks

Questions to assist in identifying risks:

- What situations represent a risk?
- What is the source of the risk?
- How can it happen?
- What could happen?
- What is the consequence if it happens?
- What is the potential cost in time, money, resources and reputation?
- Who would be affected both internally and externally?
- What controls presently exist to minimise the likelihood of the risk occurring and or the possible consequences should the breach occur?
- What controls could be implemented to minimise the risk?

Appendix five: Treating risks

Risks identified as exceeding the acceptable level should be treated. Where possible risks should be eliminated, however when this cannot reasonably occur, risks should be mitigated through reduction in likelihood and/or consequence or a transfer of the risk.

Potential risk treatment options are looked at in terms of feasibility, costs, and benefits. The option chosen should reduce the level of risk to an acceptable level or as low as reasonably practicable.

Risk treatments are captured in the risk register and monitored for progress.

Risk treatment options include:

- Reducing the Likelihood – Limiting the chance that the risk will occur by undertaking specific actions, e.g. process controls, audit and compliance programmes, preventative management, and structured training
- Reducing the Consequence – Minimising the impact of the risk, should it occur, by developing contingency plans, 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 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.

Appendix six: Monitoring and reviewing risks

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.

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

- Determining whether each risk previously identified is still relevant
- Reviewing the 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 implemented

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 Office policies, including access, equity, ethics and accountability?
- Can any improvements be made?