CITY OF MONASH

Enterprise Risk & Opportunity Management Procedures

Monash City Council

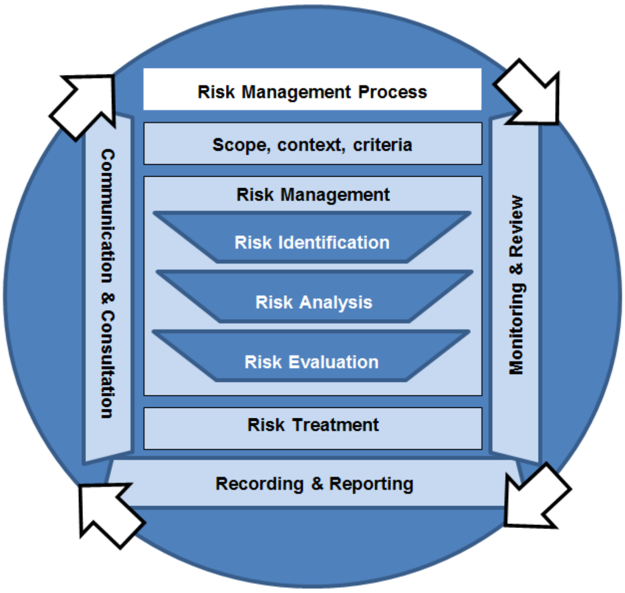
Version 1 February 2020

Contents

Purpose and principles

The purpose of the *Risk & Opportunity Management Procedures* document is to guide and support a common approach to the identification, analysis, treatment, monitoring and reporting of risk. These procedures are the "how to" element of our Enterprise Risk & Opportunity Management Framework that reflects the International Standard ISO 31000:2018, Risk management – Guidelines.

Each step in the ISO 31000:2018 process is outlined in detail along with descriptions of how and where the process is applied by Council.



Source: ISO 31000:2018, Risk management – Guidelines

The benefits of a common approach include:

- Building on existing processes to efficiently embed and strengthen risk management capabilities
- Develops a risk-aware culture
- Promotes a shared responsibility for managing risk throughout Council
- Avoids risk management being seen as an add-on activity or administrative burden.

Risk Management Process

1. Communication and Consultation

Collaboration, communication and consultation is the basis for engagement at The City of Monash. The purpose of this is to:

- Communicate and promote the awareness and understanding of risk management tools, frameworks and expectations
- Collaborate and consult with key stakeholders to obtain information that informs and supports decision-making
- Collaborate and consult with key stakeholders to identify risks and issues which could prevent the achievement of objectives

Communication and consultation takes place throughout the risk management process to ensure the right people have the right information at the right time.

Consultation can be with internal and/or external stakeholders and subject matter experts.

Consult widely in the risk management process. Bring together persons with a good understanding of the matters, projects and initiatives being assessed. This is key to obtaining insight from a variety of perspectives and a balanced view of risk, and for promoting ownership of risks.

2. Establish the Context, Criteria and Scope

CONTEXT

Establishing the context defines the basic parameters within which risks must be managed and sets the scope for the rest of the risk and opportunity management process. Council's operating environment and **context** is unique and our Enterprise Risk Management Framework (ERMF) is tailored to suit these circumstances:

- Culture and values
- Objectives, goals and strategies
- Community and stakeholder needs, expectations and partnership arrangements
- Compliance and policy obligations
- Operations, functions and services
- Economic, cultural, social and political environment

Using the Risk Categories in the risk Matrix, define the external and internal context. This will assist in the risk identification process.

CRITERIA

The risk **criteria** in our ERMF represents Council's views on the significance of risk relative to our goals and objectives. This helps us undertake a consistent approach to managing risk throughout Council. Refer to the Risk Matrix, **Impact.**

The criteria has been developed for you, see the risk matrix. Use this criteria when evaluating the level of risk

SCOPE

The **scope** of risk management activities is usually targeted towards addressing the strategic, operational and project risk profiles.

To identify the scope of the risk activity, ask the following questions:

- **What do we want to do or achieve?** What are the desired outcomes/benefits of the event, activity or project?
- **How will we know we have been successful**? What indicators, measurements or feedback will tell us we have achieved the expected outcomes/benefits of our initiative?
- **Who needs to be involved?** Who are the key internal and external stakeholders involved?
- **Which stakeholders need to be involved in the risk assessment?** Using the RACI model as a guide, who needs to be involved in the risk assessment and in what capacity?

R	**Responsible**
A	**Accountable**
C	**Consulted**
I	**Informed**

Collaborate with others to establish and document the scope of your project. The scope will identify areas of risk that could prevent the desired outcome.

3. Risk identification

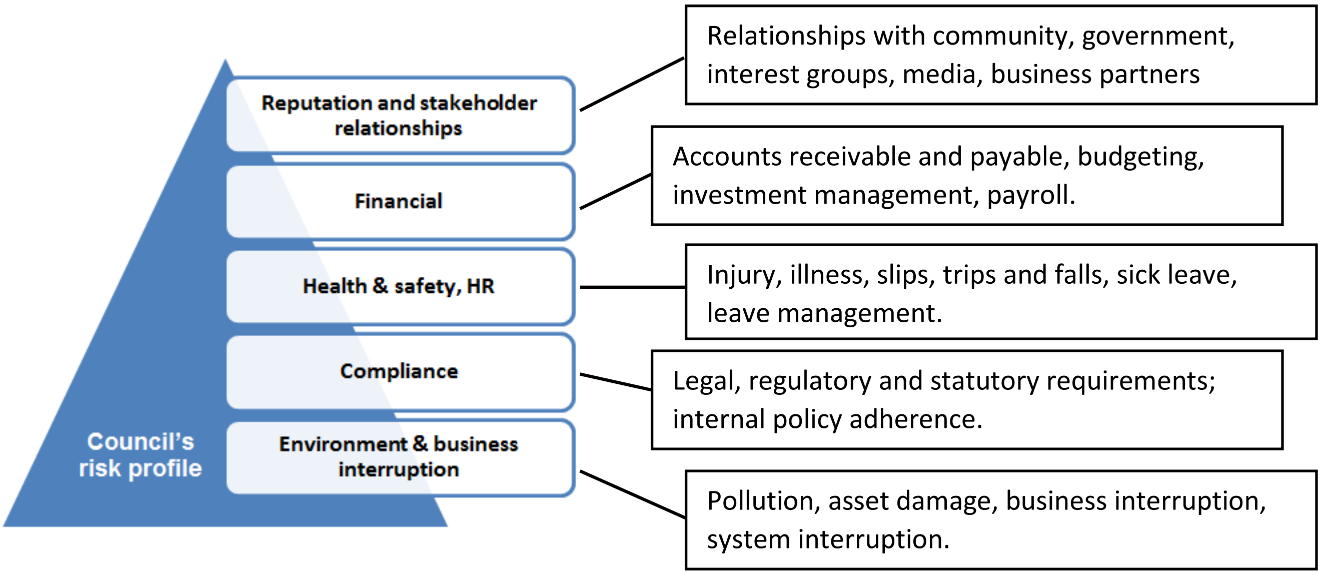
Risk identification is about finding, recognising and describing the things that can prevent us from achieving our goals and objectives. It is about asking ourselves what could go wrong and what must be right in order to achieve the objectives.

Things to consider when identifying risks:

- What could cause this strategy or initiative to fail?
- What could happen to cause embarrassment to Council, the Councillors or staff?
- Where could costs blow out or potential savings be made?
- Are we sure the idea is consistent with our mandate, policies and regulatory obligations? How do we know? Have we checked with our Legal Counsel, Chief Operating Officer or Chief Financial Officer?
- Where could there be unintended consequences on another Council initiative or division or our daily activities?
- What could be the impact on infrastructure, resourcing, IT, insurance, public perceptions?
- Do we have the right information in place to support our plan for this strategic initiative?
- How dependent is success of this initiative on the goods and services of third party providers? Are we comfortable with their capacity to deliver, as contracted?
- Where do we need to get buy-in? How do we know we will get it?
- What are other councils experiencing that can also impact this Council?
- What could happen, or is happening right now, that impacts our ability to deliver on our promises?
- What else haven't we thought of?
- What risks do we need to take to ensure we get the right outcomes from this initiative?

Council has also categorised the key areas or sources of risk particular to our operating environment. This can help to contextualise, record and report the risk. See below.

Categories of risk:


Reputation and stakeholder relationships
Relationships with community, government, interest groups, media, business partners
Financial
Accounts receivable and payable, budgeting, investment management, payroll.
Health & safety, HR
Injury, illness, slips, trips and falls, sick leave, leave management.
Compliance
Legal, regulatory and statutory requirements; internal policy adherence.
Environment & business interruption
Pollution, asset damage, business interruption, system interruption.
Council's risk profile

These five categories are listed in the risk register system and every risk is assigned to one of these categories. Where more than one category applies, the more relevant category is assigned.

The categories of risk group like sources of risk for the purpose of analysing and reporting trends, understanding the root cause of weaknesses in procedures and controls and directing risk mitigation effort towards the most significant matters.

Risk identification can be achieved through:

- Undertaking a formal risk assessment using Council's risk assessment template
- Brainstorming or workshopping a situation with key stakeholders involved in an initiative
- Consulting with subject matter experts
- Environmental scanning (see PESTLE analysis in the reporting section)
- Analysis of near miss events
- Assessing claims data

Collaborate, consult and discuss with key stakeholders and/or subject matter experts to identify risks from each category. Document these risks on the Risk Assessment Template.

4. Risk Analysis

Analysis is performed on the identified risks to determine how significant the matter is, understand how likely a risk is to occur and how large the impact would be if it did occur.

Controls are designed to reduce the likelihood of the risk occurring (preventative control) or reduce the impact of the event once it has occurred (detective and corrective controls).

Rating the effectiveness of the controls cannot be confidently known until they have been tested. This can be achieved through various mechanisms including Management review, self-assessment or internal audit.

The likelihood is described as ***the chance that something might happen.***

The Consequence is described as ***the outcome of an event and its impact on objectives.***

The Risk Rating ***provides a measure of the level of risk.***

The Risk Rating Matrix ***is a matrix that is used to obtain a risk rating by considering the likelihood against the category of consequence severity.***

Using the risk rating matrix:

The risk rating matrix is a tool designed to help analyse risks and prioritise them for treatment and reporting. It reflects the materiality of a risk in accordance with pre-defined consequence and likelihood criteria that are aligned to the categories of risk (as outlined in section 3 above). The matrix is positioned at a Council-wide level to maintain a consistent perspective of risk management across all staff and divisions.

To use this matrix, identify which category the risk falls into (financial, compliance, etc.) and the estimated impact should the risk become an event. Where available, use quantifiable evidence such as the financial impact, the number of days taken as sick leave or the system downtime, to support the analysis and estimated impact. The risk does not need to be consistent with *all* impact statements as the risk is plotted on a *best fit* basis. After the controls have been identified, estimate the likelihood of the risk occurring, this will identify the Risk Rating.

Using the Control Effectiveness table:

The control effectiveness table provides a rating of the effectiveness of the controls which is important when reporting on risks.

Risk Matrix

CONSEQUENCE	RISK CATEGORY	IMPACT	LIKELIHOOD	RARE May occur once a decade	UNLIKELY May occur in five to ten years	POSSIBLE May occur within five years	LIKELY May occur within 1-2 years	ALMOST CERTAIN May occur within next few months
CATASTROPHIC	Reputation & stakeholder relationships Financial Health & safety, HR Compliance Environment & business interruption/IT	Community, State Government and media outrage, key relationships broken down Financial impact >$5mil Fatality Regulatory investigation, legal action, fines and penalties imposed Uncontrolled spread of toxic pollutants. Building destroyed and BCP invoked. System downtime expected for >2 weeks and DR invoked		High	High	Extreme	Extreme	Extreme
MAJOR	Reputation & stakeholder relationships Financial Health & safety, HR Compliance Environment & business interruption/IT	Widespread community concern , adverse media coverage, key relationships severely damaged Financial impact $1mil - $5mil Injury or illness requires emergency response, hospitalisation Reportable breaches and regulatory investigation at Council level Spread of toxic pollutants is widespread. Building severely damaged and BCP invoked. Systems downtime is widespread and DR invoked		Moderate	High	High	High	Extreme
MODERATE	Reputation & stakeholder relationships Financial Health & safety, HR Compliance Environment & business interruption/IT	Well publicised community concern, limited media coverage and some key relationships strained Financial impact $250k - $1mil Injury or illness requires prompt first aid, medical treatment and sick leave Breach of regulatory requirement at Council level Spread of pollutants is broad but controlled. Building damage and systems interruption is localised and BCP/DR is not invoked		Moderate	Moderate	Moderate	High	High
MINOR	Reputation & stakeholder relationships Financial Health & safety, HR Compliance Environment & business interruption/IT	Community concern is voiced locally, key relationships not impaired Financial impact $50 - $250k Injury or illness requires minor medical treatment , limited sick leave In-house policy breaches by individual staff members Spread of pollutants is localised and contained. Asset or building damage and systems interruption is limited and BCP/DR is not invoked		Low	Moderate	Moderate	Moderate	High
IN-SIGNIFICANT	Reputation & stakeholder relationships Financial Health & safety, HR Compliance Environment & business interruption/IT	Negligible community concern and impact to public image Financial impact <$50k Insignificant injury, no first aid or sick leave Minor breach of in-house policy by individual staff members Spread of pollutants is minimal or tightly contained. Asset damage and system interruption is negligible		Low	Low	Low	Moderate	Moderate

Control effectiveness ratings

1	**Effective:**	Controls are appropriately designed to mitigate the risk to an acceptable level. Controls address the root causes and management has strong evidence that controls are working reliably as expected.
2	**Adequate:**	Controls are designed appropriately to mitigate risk to an acceptable level. The control is monitored on an ad hoc basis and evidence indicates the control should be working as expected.
3	**Improvement Required:**	While controls are largely addressing root causes of the risk, evidence indicates the controls are not fully implemented or are not operating reliably and hence risk is not being reduced to an acceptable level. Additional work is required to improve control implementation and reliability.
4	**Poor:**	Reviews on control effectiveness are limited or are not performed. Where available, evidence indicates that risk mitigation strategies are not working as expected due to poor control design and/or limited operating effectiveness.

Identify the controls that will assist with reducing the risk from occurring and document on the Risk Assessment Template.

Considering the identified controls, identify the likelihood of the risk occurring and the consequence level. Plot the likelihood and consequence score on the risk matrix to identify the risk rating. Document this information onto the Risk Assessment Template.

5. Risk Evaluation

Based on the outcome of the risk analysis, the purpose of risk evaluation is to determine which risks need treatment and in what priority order.

The priority for further treatment or further controls is dependent on the rating of the risk (as determined using the risk rating matrix). The course of action or escalation required correlates directly to the risk rating and is the minimum action to take. Consultation with management and other key stakeholders may identify further actions to take, depending on:

- How quickly the risk could become an event?
- Client and key stakeholder impact – could a third party in the supply chain also be at risk, emanating from our risk exposure or risk event?
- Health and safety at risk – is the health and safety of Council staff, contractors, volunteers and visitors at risk?
- How widespread is the risk across council departments and activities?

The risk escalation criteria outline what course of action is required, when it is to commence and the level of management involved. This forms the baseline for developing the risk treatment plan (see risk treatment section below).

Risk escalation criteria

	Risk tolerance and escalation	Risk treatment and monitoring
Extreme	Risk is far outside of tolerance levels. Escalate immediately to executive management.	Requires immediate treatment to commence within 1 week, with ongoing executive oversight.
High	Risk is outside of tolerance levels. Escalate promptly to senior management.	Requires prompt treatment to commence within 2 weeks, with ongoing senior management oversight.
Moderate	Risk is on the tolerance boundary. Escalate to management.	Treatment plan to commence within 4 weeks with regular oversight from senior management.
Low	Risk is within tolerance boundaries but outside of the preferred operating range.	Treatment options and oversight plan to be developed with management.

Council's appetite for risk is also considered at this point. For example, if the assessed level of risk is within risk tolerance boundaries, the decision may be to do nothing further.

6. Risk Treatment (additional controls)

When determining an appropriate risk treatment in accordance with the risk escalation criteria, consider the cost versus benefits:

- Do the costs (financial, effort, resources, etc.) justify the benefit?
- What is the cost of not treating the risk?
- Could there be unintended consequences of actually implementing the treatment activity that result in another risk or cost?
- Is the treatment consistent with Council's policies, obligations, values, culture and mandate?

Keeping the above in mind, the **risk treatment options** are to:

Decision	Indicators
Remove or avoid the risk	Remove the risk by not proceeding with the policy, program or activity or choose an alternate means of action.
Retain or accept the risk	Council has made an informed decision not to treat the risk, because: a) The cost of controlling the risk outweighs the benefits, or b) There are no appropriate controls available to reduce or eliminate the risk. Where any risk ranked low or above are accepted, justification of acceptance is required and a record included in the risk register system.
Treat the risk	Apply controls or other mitigating activities designed to reduce the likelihood and/or consequences of the risk event occurring.
Transfer or share the risk	Share the responsibility with another party such as an insurer/contractor who shares the loss if the risk event were to occur.
Increase the risk	Consciously take on risk to pursue an opportunity and achieve desired outcomes of a strategy, project or initiative.

Risk treatments or additional controls are recorded in the risk register as *Additional Tasks* and should include the following information:

- What is the treatment activity and how will it reduce the risk likelihood and/or consequences?
- Who is responsible for completing the treatment activities?
- When will the treatment be completed?

When developing additional controls, identify who is the Task owner, the completion date and reporting expectations.

7. Recording and reporting

Recording risks

Each stage of the Risk Management Process must be recorded to ensure:

- There is sufficient information to demonstrate how risks have been managed using the ERMF. This is guided by the mandatory fields to be populated in the risk register system.
- Decisions to treat or not to treat risks are clearly supported.
- Key information is readily accessible and reporting risk to senior stakeholders is targeted and insightful.

The corporate system used to record Strategic and Operational risks is Pulse.

The corporate system used to record project risks is Our Project Place.

Reporting risks

The purpose of reporting risks is to provide sufficient information to help management understand what can impact or prevent the achievement of objectives/benefits. Reporting may also identify the opportunities Council needs to take (which includes taking on risk), to achieve objectives.

Frequency:

It is expected risk registers are reviewed and reported quarterly.

Outcome:

Management use this information to understand how well risks and their controls are being managed and what further needs to be done, if anything, to address the identified risks, and then decide:

- What must we start doing?
- What must we stop doing?
- What must we keep doing?

When reporting on risks, consider the following:

Changes to the risk register

A summary of what has been added or archived from the register and why; what ratings have changed and why. This may be as a result of risk treatment (controls) activities, control assessments or a change in the operating context.

Status of the higher rated risks

These are the High and Extreme risks. How effective are the controls? How have risk treatments progressed and how has this reduced the current level of risk? How do we know how well treatments (such as application of new treatments and/or risk controls) are working? What testing has occurred on the controls?

If the consequence or likelihood of the risk occurring has heightened, and greater management effort is required to mitigate the risks, this is the key opportunity to explain what has happened and what this means to Council.

Risk environmental scan

New and emerging risks can be assessed through an environmental scan such as a PESTLE analysis. This is a tool for researching and generating insight around the internal and external environment that Council needs to be aware of before they become risks and potential loss matters.

P	E	S	T	L	E
Political	Environmental	Social	Technological	Legal	Economic

From research into each element of the PESTLE tool, insight is developed to ascertain what new or emerging trends, events and scenarios have been identified, how quickly could a risk become an event, and what does this mean for Council?

Project risks and trends

Project risks are usually reported by the Project Control Group (PCG). There may be occasion where risk trends across multiple projects are reported to The Executive Leadership Team and the Audit and Risk Committee as the collective implications of the risk trend may be significant.

Analysis of like risks, risk events and near misses

Analysis and reporting of like risks (as identified through their risk category, control type or any other field from the risk register system) is valuable as it can identify thematic issues that together can represent matters of significance.

Analysis of **risk events and near misses** is pertinent to understand the root cause of the matter and what has been done to prevent similar events from occurring. This may be done on a trend basis or targeted towards higher-rated risk, which is consistent with the tone and messaging of the report and the seniority of the report readers.

8. Monitoring and review

Monitoring of the enterprise risk management (ERM) processes is performed to ascertain that:

- The risk management tools and mechanisms are working effectively
- The ERM processes remain fit for purpose
- Risk management outcomes are generating information that is valuable, insightful and helps management to address the effects of uncertainty and to make decisions based on the best available information.

Oversight of the ERM activities is performed by The Executive Leadership Team and by the Audit and Risk Committee whose responsibilities are outlined in the Audit and Risk Committee charter. The following reports can be developed to assist The Executive leadership Team and Audit and Risk Committee to discharge their oversight responsibilities.

Risk assurance review outcomes

As Council operates a *three lines of defence* model (described in the ERMF document), sharing information between the three lines is key for integrating risk management activities. Assurance is obtained from internal audit reviews and any other reviews performed by management or the second lines functions (for example a compliance review). The outcomes of these reviews provide insight around the effectiveness of risk controls and the adequacy of governance and risk management activities within Council operations. A summary of this insight is reported periodically to Council's senior leaders. Assurance review outcomes are also recorded in the risk register system and risk control ratings are updated as *Effective; Adequate; Improvement required; or Poor*, in accordance with the *Control effectiveness ratings*.

Risk integration activities

There are 17 areas where risk management practices are integrated into Council's daily activities (see page 9, ER&OM Framework - 2-Integration).

A key benefit of integrating risk management into daily processes is that it broadens the scope and opportunity for risk management activities to be practiced and embedded throughout the organisation. It helps to strengthen risk capability amongst staff, builds stronger risk insight and helps to manage the effects of uncertainty in Council activities.

On a periodic basis it is prudent to confirm that risk management processes are appropriately embedded into the daily activities and that these are operating effectively. A report on the status of risk integration practices provide Executive management and the Audit and Risk Committee an overview of Council's risk maturity and may also identify opportunities for resources to be directed towards strengthening risk maturity and capability.

The risk integration assessment can be performed:

- Informally through discussion during the semi-annual operational risk profiling process, as key managers are usually present at these meetings, or

- As part of a targeted second-line risk management review designed to strengthen risk processes and controls. This is an effective way to provide management with assurance over key processes. Such reviews may inform the design of the internal audit plan.

Where gaps or weaknesses in the integration of risk management practices are identified, there is an opportunity for processes and controls to be strengthened. The risk team can work together with management to help strengthen control design and embed these into processes.

Risk definitions

Term	Definition
Consequence	The outcome of an event affecting objectives that can be either positive or negative. This can be expressed either quantitatively (e.g. in financial terms) or qualitatively (e.g. being a loss, injury, disadvantage or gain).
Control	The measure to modify a risk that can include any policy, procedure, practice, process, technology, technique, method, or device that modifies or regulates risk.
Current level of risk	The level risk at a point in time, based on the known level of control effectiveness, and rated against the risk rating matrix.
Event	An occurrence or something that has happened that has both a cause and a consequence. By comparison, a risk has not happened, but *could* happen.
Internal audit	An independent, objective assurance and consulting activity that brings a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, controls and governance processes. (Source: International Professional Practices Framework [IPPF], The Institute of Internal Auditors Research Foundation. Florida, USA, January 2011).
Likelihood	The chance or probability of something happening. This can also be expressed quantitatively or qualitatively.
Near miss	An event without consequences.
Operational Risk	The risk of loss resulting from inadequate or failed internal processes, people and systems.
Project Risk	An uncertain event or condition that, if it occurs, has a positive or a negative effect on a project’s objectives.
Risk	Defined as the effect of uncertainty on objectives. • An effect is a deviation from the expected which can be positive or negative. • Objectives can have different aspects, (such as financial, health and safety, technology and environmental goals) and can apply at different levels (such as organisation-wide, operational, project, product and process) • Risk is usually expressed in terms of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.
Risk Appetite	The amount of risk that an organisation is prepared to accept in the pursuit of objectives.
Risk Culture	The behaviours, attitudes and awareness that determine how people think about and manage risk.

Term	Definition
Risk Governance	The monitoring and oversight arrangements in place to oversee application and effectiveness of measures to manage risk.
Risk Management	Coordinated activities to direct and control an organisation with regard to risk.
(Enterprise) Risk management framework (ERMF)	A set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.
Risk Program of Work	The basis upon which risk management practices will be performed and integrated throughout an organisation. Also known as a risk plan or risk strategy.
Risk profile	A written description of a set of risks.
Risk register	A record of information about identified risks
Risk register system	Usually an electronic system or software program used to store the risk profile. Also often known as a *governance, risk and compliance* (GRC) system.
Risk tolerance	The range or maximum level of risk an organisation is prepared to accept in the pursuit of objectives.
Risk Treatment / Action Plan	The process to modify risk that can include avoiding, reducing or increasing risk taking activities.

Appendix A: Risk Assessment Template

						With existing controls							With additional controls			
Risk ref	**Category of risk**	**Risk description**	**Causes**	**Existing controls in place**	**Owner of control**	**Consequence**	**Likelihood**	**Risk Rating**	**Additional Control to be developed and implemented (task)**	**Owner of task**	**Target date for development and implementation**	**Completion date**	**Consequence**	**Likelihood**	**Residual Risk Rating**	**Control effectiveness**