Insurance Commission
of Western Australia

RiskCover

Risk Management Guidelines

Contents

1. Introduction

These guidelines have been produced by RiskCover to assist the Government of Western Australia's agencies (agencies) in developing and implementing effective risk management processes. They should be read in conjunction with the WA Government Business Continuity Guidelines, as the management of critical incidents and emergencies is just one aspect of an agency's overall approach to managing risk.

> "*All public sector bodies should manage the risks associated with the activities performed by their organisation. This involves prudently conducting risk assessment processes to identify the risks facing organisations, being able to demonstrate the management of risks and having continuity plans to ensure they can respond to and recover from any business disruption.*
>
> *Public sector bodies should ensure policies and continuity plans are maintained to ensure they are up to date with the activities performed by their organisation.*
>
> *Risk management is essential to the optimal operation of the public sector, as articulated in Treasurer's Instruction 825 Risk Management and Security.*
>
> *Planning for major risks, such as natural disasters, terrorism and health pandemics among others are matters of good corporate governance aimed at ensuring that the public sector and the community are well prepared for emergencies of any kind.*
>
> *Risk management consultancy services can be sourced via the Department of Finance's Common Use Arrangement 23706 – Audit Services and Financial Advice."*
>
> *M C Wauchope, Public Sector Commissioner*

The Public Sector Commissioner's Circular 2015-03 Risk Management and Business Continuity Planning provides guidance on agency responsibilities.

The International Standard AS/NZS ISO 31000:2009 provides the principles and general guidelines to be considered when developing risk management frameworks and programs.

2. Definition of Risk

The AS/NZS ISO 31000:2009 definition of risk is “the effect of uncertainty on objectives”.

Risk manager should consider the possibility of risks occurring and should apply risk treatment options to ensure that the uncertainly of their agency meeting its objectives will be avoided, reduced, removed, modified and/or retained.

3. Principles of Risk Management

3.1. Creates and protects value

Good risk management contributes to the achievement of an agency’s objectives through the continuous review of its processes and systems.

3.2. Be an integral part of organisational processes

Risk management needs to be integrated with an agency’s governance framework and becomes a part of its planning processes, at both the operational and strategic level.

3.3. Be part of decision making

The process of risk management assists decision makers to make informed choices, identify priorities and select the most appropriate action.

3.4. Explicitly address uncertainly

By identifying potential risks, agencies can implement controls and treatments to maximise the chance of gain while minimising the chance of loss.

3.5. Be systematic, structured and timely

The process of risk management should be consistent across an agency to ensure efficiency, consistency and the reliability of results.

3.6. Based on the best available information

To effectively manage risk it is important to understand and consider all available information relevant to an activity and to be aware that there may be limitations on that information. It is then important to understand how all this information informs the risk management process.

3.7. Be tailored

An agency’s risk management framework needs to include its risk profile, as well as take into consideration its internal and external operating environment.

3.8. Take into account human and cultural factors

Risk management needs to recognise the contribution that people and culture have on achieving an agency's objectives.

3.9. Be transparent and inclusive

Engaging stakeholders, both internal and external, throughout the risk management process recognises that communication and consultation is key to identifying, analysing and monitoring risk.

3.10. Be dynamic, iterative and responsive to change

The process of managing risk needs to be flexible. The challenging environment we operate in requires agencies to consider the context for managing risk as well as continuing to identify new risks that emerge, and make allowances for those risks that no longer exist.

3.11. Facilitate the continual improvement of organisations

Agencies with mature risk management culture are those that have invested resources over time and are able to demonstrate the continual achievement of their objectives.

4. Risk Management Process

4.1. Step 1: Establish the Context

There are two elements in this step:

1. Setting the overall agency context and
2. Establishing the specific risk assessment context.

As part of setting the overall context, the organisational-wide framework which risk management will take place is defined and the tolls to measure and assess risks within that overall context are developed. The specific context then defines the framework of any specific risk assessment exercise with the agency**.**

4.1.1 Overall Agency Context

An agency's risk management program should be aligned to its strategic objectives and is most effective when it is integrated with the overall planning and management functions of the organisation.

In developing a framework for managing risk, an agency needs to consider the following:

- Core purpose, vision, mission and values – why does it exist? Strategic direction, goals, required outcomes and deliverables. These may be defined by legislation, ministerial directive, charter, etc.
- Internal and external environments, often assessed using a SWOT analysis.
- Internal and external stakeholders – who are they, what are their needs and expectations?
- Organisational planning, reporting and management processes.

Based on the outcome of this analysis, an agency will then be in a position to define how risks are to be managed across the organisation, through the development of:

- A risk management policy.
- Risk management guidelines or procedure, which clearly defines how the risk management process is integrated into the planning, delivery, monitoring and reporting activities of an agency
- Risk reference tables, used in the evaluation of the risk and also of any existing controls. They also include a definition of the acceptance and reporting criteria for specific levels of risk.
- Risk management implementation strategy – a plan of how the policy and guidelines are to be communicated and implemented.

Risk Reference Tables

Risk reference tables are developed by an agency for the purpose of establishing guidance as to how risks are to be evaluated, assessed, measured, accepted and reported within an agency. As well as establishing a common language, the use of semi-quantitative measures removes some of the subjectivity of the assessment process and allows risks from any part of the agency to be compared with any other, and hence prioritised.

There are commonly four different tables used:

a. Consequence or impact table
b. Likelihood table
c. Existing controls rating table
d. Risk acceptance criteria table

a. Consequence or Impact Rating Table

Consequence categories are based upon the individual agency's criteria for measurement of success and should reflect the agency's economic, social and in some cases, environmental responsibility.

The categories should include those key areas, which, if impacted upon, would have a significant effect on the ability of the agency to achieve its goals. In government, these impact areas are often defined as 'financial', 'injury', 'service interruption', 'reputation and image', 'KPIs or key objective/deliverables' and depending on the nature of the organisation, 'environment'.

Consequences are usually rated on a scale of 1 to 5, 1 being insignificant and 5 being catastrophic. This is generally referred to as level of the consequence. For each of the consequence categories defined, an agency needs to develop criteria for each of the impact levels specified. Care must be taken to ensure that impact criteria relating to different categories are equivalent at the same level of consequence, for example the definition of catastrophic financial loss needs to be equivalent in terms of priority as the definition of, a catastrophic reputation and image impact.

b. Likelihood Rating Table

The other measure of risk is likelihood, and this is also commonly measured on a scale of 1 to 5, with 1 being very unlikely and 5 being almost certain. Likelihood can be considered in two aspects. In one sense, you can base the scale on how frequently a given consequence will (or is likely to) happen, for example more than twice per year, every year, every three years, etc. Alternatively, you can consider the probability of something happening in a defined forward timeframe, for example in the next five years as a consequence is almost certain, probable, possible etc. In either case, each level of the scale should be quantified.

Each risk is first analysed and evaluated in terms of the potential consequences resulting from a particular risk scenario. Then the consequence of this scenario, with the associated level of likelihood, is rated. Using 1 to 5 scales for consequence and likelihood results in a level of risk ranging from 1 to 25.

The level of a risk varies as you consider the context of how that risk is being managed. All risks will have an inherent level of risk. This is defined as the level of risk with no formal controls in place, or the level of risk in the event of a breakdown of all controls. Some organisations choose to assess and document this level of risk prior to considering the effectiveness of existing controls. Having information available which relates to this inherent risk level means that, when considering the adequacy of controls, the inherent or worst-case scenario is known.

Once the existing controls have been documented and assessed for effectiveness, the assessed level of risk can be evaluated. This is the level of risk with current controls in place.

Should the assessed level of risk be unacceptable, then additional controls or improvements to existing controls, in the form of Treatments, are put in place. In order to evaluate the cost benefit of these proposed actions, a predicted level of risk is estimated. This is the predicted level of risk after the treatment plan has been implemented.

Finally, once a risk treatment plan has been implemented, the risk is once again evaluated and a residual level of risk is calculated. This is the remaining level of risk exposure and should now be in a range that is acceptable to the agency.

c. Existing Controls Rating Table

A control is an established mechanism, procedure, process or practice that is used to manage a risk. It controls the risk by reducing its consequences, likelihood, or both. We say controls are in place when they are being actively applied or practiced.

This table is used to rate the adequacy of existing controls that are currently applied to a particular risk. It is usually qualitative.

This is a reasonableness test. Is the agency doing what is reasonable in the circumstances to reduce the likelihood and/or consequences of this risk?   There may be several controls, each of which goes some way towards reducing the risk. What you are rating is the adequacy of those combined measures.

d. Risk Acceptance Criteria Table

This table defines the agency’s risk tolerance, or risk appetite and gives guidance as to the acceptability of risk. For a given level of risk, the table defines how that risk is perceived (low, moderate, high, or extreme) and may specify the level of controls rating that is necessary to accept the risk. The criteria often defines how risks are to be reported, reviewed and who is the accepted decision-maker.

4.1.2 Specific Risk Assessment Context

Once the overall agency context is established, the requirements for a specific risk assessment exercise can be defined. For instance, you may be embarking on a new strategic planning cycle and wish to integrate the identification, assessment and management of risks as part of your strategic planning function. For each individual risk assessment exercise, it is important to ascertain the following:

- Set the parameters: what is the specific subject of the assessment?
- Identify the essential stakeholders who need to be involved in the assessment.
- Ensure all workshop participants are clear about the purpose of the assessment.

The specific risk assessment context can be categorised as strategic, operational, or project:

Strategic: Strategic risks concern the whole of the agency. They are the risks associated with long term organisational objectives and the means by which those objectives will be achieved. Strategic risk assessment is normally conducted at a board or executive level and is most effective when integrated with the strategic planning process.

Operational: Operational risks are associated with the development and implementation of operational plans. They are the risks associated with your normal business functions. Operational risks should be assessed by the parties familiar with the particular function or service with which the risks are associated.

Project: Project risks are associated with specific projects or discreet undertakings. Any project will go through a life cycle, for example, conception to planning, scoping, contracting, design, construction, testing/commissioning, handover and operation. Project risks exist at every stage, and they need to be identified and managed to ensure the successful completion of the project.

Once the context for a particular risk assessment has been specified, and the particular strategy, activity or project defined, the next step is to identify the critical success factors and key dependencies associated with it.

A critical success factor is defined as any essential resource, expertise, input, or other factor, which is critical to the success of that particular strategy or activity. A key dependency is relationship with, or reliance upon, another person, section or organisation whose input is vital to a successful outcome. These success factors and dependencies become the basis to identify risk; anything that has a negative impact upon them constitutes a risk to the desired outcomes.

4.2. Step 2: Risk Identification

4.2.1 What is a Risk?

The identification process considers each strategy, activity or function, as defined by the context set in Step 1, looks at what is critical to the success of that strategy, activity or function, and then considers what may go wrong. This is defined as the risk.

Do not mistake risks with the consequences. 'Injuries', 'Financial Loss' and 'Reputation Damage' are not risks but consequences of a risk, that is, if your risk was to eventuate, it could result injuries, financial loss and/or reputation damage.

For each risk, you should identify possible causes of the risk event. Each risk may have one or more causal factors which can either directly or indirectly contribute to the risk even occurring. Identifying the range of causes will help you to better understand the risk, evaluate the adequacy of existing controls and design effective risk treatments.

4.2.2 Categorisation of Risk

a. Source of Risk

A useful approach to help identify any common causes of risks across different areas of an organisation is to categorise the risks by 'source of risk'. This facilitates the reporting and management of those systemic issues allowing common causes to be managed with agency-wide controls or treatments, rather than at an area or department level.

b. Impact Range

Another way to categorise risks is by impact range. The impact range is a classification hierarchy which indicates how wide the consequences of the risk will reach, within the organisation and beyond.

4.3. Step 3: Risk Assessment – Analysis and Evaluation

In general, agencies already have a broad range of public sector procedures and systems in place that act as risk controls. As a result, the assessment process used by most agencies takes into account the effectiveness of these existing controls. Therefore, in this context, risk assessment involves:

- Identifying and evaluating any existing controls.
- Analysing the risk in terms of consequences and likelihood.
- Evaluating the level of risk against a pre-defined acceptance criteria.

4.3.1 Existing Controls and Controls Assurance

Controls are the measures that are currently in place, at the time of the risk assessment, that reduce the likelihood and/or consequences of the risk.

The adequacy of the controls is assessed on a common sense, qualitative basis. This can be viewed as a reasonableness test; are you doing what is reasonable under the circumstances to prevent or minimise the impacts of the risk? The recommended rating scale is as follows:

Excellent - Doing more than what is reasonable under the circumstances.
Adequate - Doing what is reasonable under the circumstances.
Inadequate - Not doing some or all of the things that would be reasonable under the circumstances.

While it is relatively easy to identify and rate controls in a workshop environment, this does not necessarily ensure those controls are effective and being used in reality. It is essential to have a controls assurance process as a means to confirm their existence and effectiveness, and in doing so, consideration should be given to factors such as:

- Is the control relevant?
- Is the control documented?
- Is the control in use?
- Is the control up to date?
- Is the control effective?

If an existing control is identified as being ineffective, then the necessary improvement should be incorporated into a treatment action plan.

The review and sign off of existing controls is an integral part of the management of the risk; responsibility needs to be assigned to ensure there is accountability for and ownership of this important aspect of the risk management process.

4.3.2 Risk Analysis

This is the process of considering the consequences and likelihood of a particular risk scenario to determine the level of risk, using the risk reference tables developed as part of setting the organisational context.

Consequence Rating

A risk that eventuates may impact an agency across a number of difference areas, to a greater or lesser extent. When analysing the consequences of a risk event, an agency needs to consider the level of impact (1 to 5) in relation to each of the consequence categories defined in the consequence table. For example, a risk may have an impact of 5 for financial loss and 4 for reputation and image and little or no impact in other areas. Both ratings may be recorded, but the overall level of risk calculation is based on the highest value, which in this case is a 5.

Likelihood Rating

This describes how likely it is that a risk will eventuate with the defined consequences. Likelihood can be defined in terms of probability or frequency, depending on what is most convenient for the agency's purposes.

Calculating the Level of Risk

The level of risk or risk rating, is calculated by multiplying the consequence and likelihood ratings. For any risk, there may be a number of different likelihood/consequence scenarios across the different risk categories and, within each category, ranging from 'likely but not serious' to 'less likely but more serious'. It is important to rate the realistic worst case scenario, which is the worst case level of risk considering both consequences and likelihood. In some cases, you may consider the same consequence category more than once for the same risk, in order to calculate the real worst-case scenario. Where there are multiple ratings for a risk, the highest combination of consequence/likelihood is taken as the final rating.

4.3.3 Risk Evaluation

Once the level of risk has been determined, the next step is to evaluate the risk and see where the risk fits against the agency's overall risk criteria.

4.3.4 Risk Ownership and Risk Decision

Each risk that is identified needs to be allocated a risk owner. This is the person responsible for managing the risk, and is usually the person who is directly responsible for the strategy, activity or function that relates to the risk. Some of the key responsibilities of the risk owner include:

- Sign-off on acceptance of the risk
- Responsible for the regular review of the risk
- Responsible for the regular reporting on the risk
- Monitoring of controls
- Implementation of any risk treatments

Assigning risk ownership ensures a specific person is responsible and accountable for a particular risk. It is usually impractical and ineffective for risk ownership to be assigned to a body, such as a business unit or committee.

Once a risk has been analysed and evaluated, the risk owner makes an informed decision to do one of the following:

- Accept the risk – the reward outweighs the risk and the existing controls meet the criteria specified in the risk acceptance criteria table.
- Avoid the risk – do not carry on with the activity that is associated with the risk.
- Treat the risk – reduce either the likelihood, consequence or both by improving existing controls or adding new controls, so that the risk can be accepted.

The risk decision balances the issues of risk and reward. Should an opportunity be passed over because of the risks associated with it? Should more be done to manage the risk so as not to miss out on the opportunity? These are questions that the agency will need to address. An organisation cannot progress or improve without capitalising on opportunities, and opportunities will always have associated risks. The risk management process allows you to optimise these decisions and demonstrate you are effectively managing the risks.

4.4. Step 4: Risk Treatment

In the previous step, risks were assessed and decisions were made to accept them or not. In practical terms, risk avoidance, that is ceasing the activity that creates the risk, is rarely a practical option. Agencies normally have their activities define by a higher authority and if there are risks associated with those activities, a way must be found to manage them.

In some cases, existing controls will be deemed to be adequate and effective, and the risk will be accepted as it stands. In other instances, the risk will need to be more effectively managed before it can be accepted. This latter case requires the formulation of risk treatments. Risk treatment involves identifying a range of options to reduce the consequences and/or likelihood of a risk, or improve the controls rating, evaluating those options, preparing treatment plans, and implementing them.

4.4.1 Identify, Evaluate and Select Treatment Options

Each unacceptable risk will have a number of treatments. Other than the option of avoiding the risk entirely, treatment options will do one or all of the following:

- Reduce the likelihood of the risk eventuating.
- Reduce the consequences of the risk if it eventuates.
- Improve the controls rating to ‘adequate’ or ‘excellent’.

Managing risk is about doing all things reasonable, not all things possible. To evaluate the treatment options a number of selection criteria can be applied:

How will the treatment impact the level of risk? For each treatment option, a predicted level of risk should be calculated considering the impact of adding this option as a new control. Treatment options, which reduce the level of risk to an acceptable level, should be considered.

Cost of implementation versus benefits derived: Selecting appropriate options involves balancing the cost against the benefits derived. An option may appear to be the best option from a risk reduction perspective, but the cost of implementation may be prohibitive.

Compatible with agencies objectives: The options selected need to be compatible with the overall objectives of the agency. Treatments that are incompatible with existing objectives, culture, or policies are obviously unacceptable, no matter how effective they might prove.

4.4.2 Prepare and Implement Treatment Plans

The purpose of the treatment action plans is to document how the chosen options will be implemented. These plans should include the following:

- Proposed actions – what is the selected treatment?
- Resource requirements – what is required to implement the treatment?
- Responsibilities – Who has responsibilities to implement the treatment (treatment owner)?
- Timing – What are the timeframes for treatment implementation?
- Performance measures – What are the key indicators that will demonstrate the progress of implementation and ultimately the effectiveness of the treatment option?
- Reporting and monitoring requirements – Who needs to be informed during and at completion of the implementation of the treatment? How will the implementation be monitored?

A treatment becomes a control only when it has been 100% implemented and signed off by the treatment owner. It is then subject to controls assurance and the regular monitoring and review process. Following the implementation of the treatment options, the level of risk needs to be re-evaluated to determine if the treatment brings the risk to an acceptable level for the agency. If not, further treatment options may need to be selected.

5. Monitor and Review

Monitoring and reviewing is an ongoing part of risk management that is integral to every step of the process. It is also the part of risk management that is most often given inadequate focus, and as a result the risk management programs of many agencies become irrelevant and ineffective over time. Monitoring and reviewing ensure that the important information generated by the risk management process is captured, used, and maintained.

Monitoring and reviewing are related processes, but the distinctions between them are important in the context of risk management.

- **Monitoring** is an ongoing process of routine surveillance of both internal and external environments.
- **Reviewing** is a more periodic process that looks at the current status or situation, and is usually has a specific focus.

Monitoring and reviewing should be designed to detect both gradual and sudden change. Continuous monitoring is most likely to detect a dramatic change in a timely fashion, whereas periodic review of a particular aspect of the risk process is more oriented towards detecting trends and incremental change.

5.1. Focus Areas

Monitor and review procedures are focused on two principle areas of risk management.

The first area relates to issues specific to a particular risk assessment, which would cover the following:

Context: **T**he risk assessment context, which was established from a number of facts and deductions. For instance, the operational environment, agency structure, stakeholder expectations, statutory requirements, economic conditions and political environment are all based on perceptions at the time. The monitoring and review process should detect if any of these underlying assumptions have changed, or if new factors have emerged that impact upon the context of the particular risk assessment.

Risks and controls: Numerous factors can cause the likelihood and consequences of risks, or the actual nature of the risks themselves, to change. The controls for risks can also become less effective or irrelevant. Monitoring by the risk owner and others will ensure the timely detection of these changes so that appropriate action can be taken.

Treatments: Risk treatments need to be monitored and reviewed to ensure they are fully and correctly implemented. In some cases, treatments need to be adapted or strengthened because the risk they are designed to address has changed; in other instances, resources can be saved by discontinuing irrelevant treatments.

The second area for monitor and review is the application of the risk management process across the entire agency, with specific attention to the following:

- Consistent application of the risk management process across the agency.
- Incorporation of the risk management process into strategic, operational and project/event planning.
- Adoption of risk management practices and procedures by staff at all levels.

5.2. Risk Management Performance Measures

To be able to effectively monitor and review the management or risk within an agency, appropriate performance indicators need to be developed. These may be outcome based or process based. Outcome based performance indicators by their nature, lag the event. This is, the measurement is generated some time after the event that caused it. For instance, a report on claim costs would not be available until quite some time after the incident that gave rise to the claim. However, outcome performance indicators tend to be relatively accurate and sensitive, so they are often more appropriate for measuring gradual change. Process performance indicators measure activities and processes as they occur and thus provide more timely, if less precise information about changes. For instance, an overtime report could provide an indication that staff are over extended or the agency is under resourced. They generally do not provide precise information about the nature of the problem, but it is timely.

5.3 Roles and Responsibilities

The monitor and review of an agencies risks is an integral part of all core business functions, and it should be seen and treated as such.

The monitor and review of the specific risk contexts, actual risk, controls and treatment is primarily the responsibility of risk and treatment owners and be should be integrated into the existing reporting lines and forms of the agency.

The monitoring and review of the application of the agency's risk management policy and procedures should be integrated into the role of senior management, who should then ensure that the process is effective in delivery the desired outcomes. Internal and external audit may also play an important part in verifying application of the risk management process.

Risk management should be fully incorporated into the operational and management processes at every level of the organisation.

A final comment with regard to monitor and review is the important role it plays in good corporate governance. All agencies face increasing requirements for sound and transparent decision making and prudent allocation of resources. The monitoring and review process is pivotal in fulfilling these requirements. A structured risk management process provides a means for senior executives and directors to stay informed about those risks. It contributes transparency and objectivity to decision making, and it provides an audit trail to determine how those accountable officers have fulfilled their obligations to provide good governance.

6. Risk Management Implementation

The key steps in implementing a risk management process within an agency are summarised below:

1. Support of Senior Management

This involves the development of an organisational risk management philosophy and awareness of risk at senior levels and includes the nomination of an executive sponsor who will act as a champion of the process, and a Risk Management Coordinator who will assist the sponsor by facilitating the process.

2. Development of the Risk Management

The risk management framework defines the context for managing risk within an agency as discussed in Step 1. It includes a risk management policy and risk reference tables.

3. Communication/Education

A program of staff education and communication needs to be developed which includes:

- Dissemination of the policy and procedures.
- Raise awareness about managing risks.
- Deliver education session on the specifics of the process.
- A performance management process.
- A process for recognition, rewards and sanctions.

4. Managing Risks at the Strategic Level

The next step in the implementation is to develop the program to identify, assess, treat, monitor and report on strategic risks as an integrated part of the strategic management process.

5. Managing Risks at the Business Unit Level

Develop the program to identify, assess, treat, monitor and report on operational or project risks as an integrated part of the existing business unit management process. This may run concurrently with the strategic risk management program.

6. Monitor and Review

- Develop indicators – to measure the performance of the risk management process.
- Risk reporting – establish the process for Business Units to report on their risks and progress of treatments.
- Link incident and accident reporting mechanisms to the risk management process.
- Risk auditing – develop links to the internal audit process to ensure that the risk management process is efficient and effective in meeting the objectives set out in the policy and that key organisational risks are being managed.