Undertaking the Risk Management Process

Audience

This information sheet is intended to assist Commonwealth officials at the Generalist and Specialist levels understand the process of:

- establishing the context of your internal and external operating environments,
- identifying, analysing, evaluating and treating your risks,
- communicating and consulting on your risks,
- monitoring and evaluating your risks, and
- recording and reporting your risks.

At a glance

This information sheet utilises the *AS/NZS ISO 31000:2018 Risk Management – Principles and Guidelines* as its foundation. It is noted that ISO guidance is not the only way to approach the risk management process, nor is Comcover requiring, prescribing or mandating alignment with the ISO31000:2018.

The AS/NZS ISO 31000:2018 Risk Management – Principles and Guidelines (refer to Diagram 1) recommends that risk management be based on three core elements:

1. A set of principles that describes the essential attributes of good risk management, which support the creation and protection of value.
2. A risk management framework that provides a structure for risk management within an entity or activity that is underpinned by leadership and commitment.
3. A risk management process that prescribes a tailored, structured approach to understanding, communicating and managing risk in practice.

It is important that a risk practitioner understands the importance of how the risk management process fits within the broader risk management framework and principles.

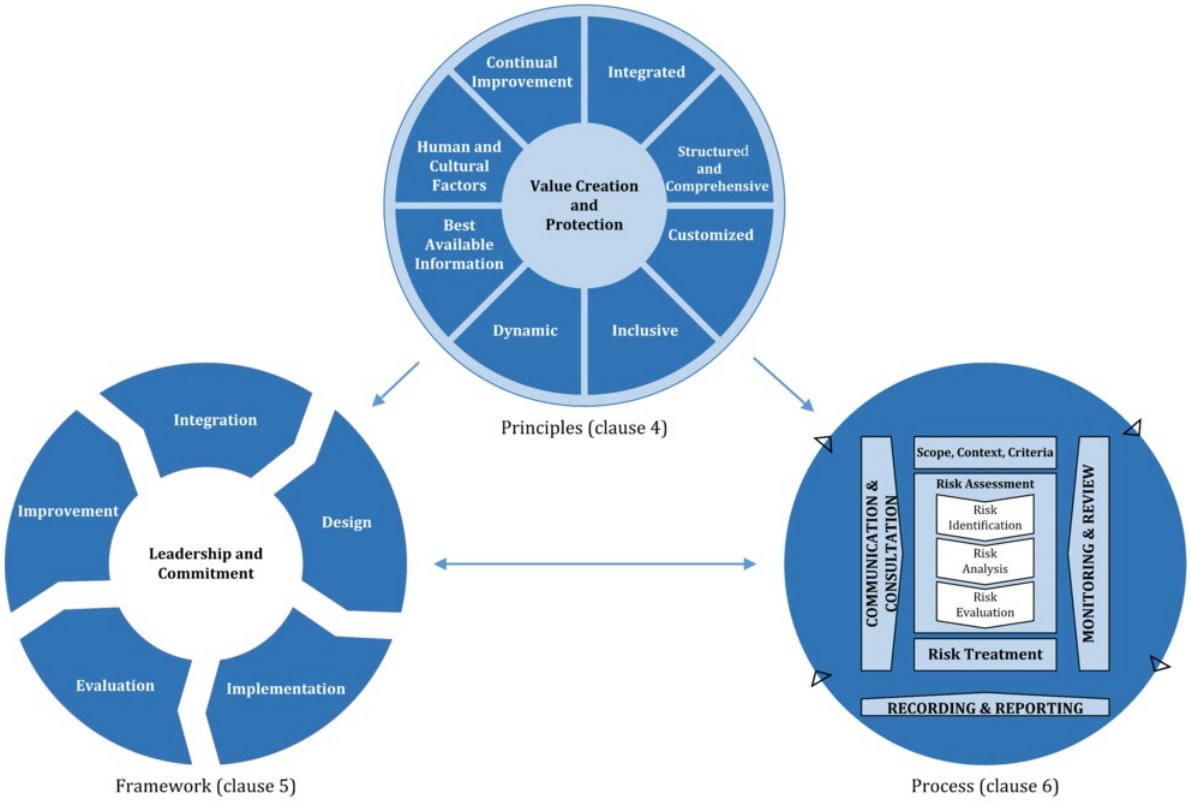


Diagram 1: Source - IS0 31000:2018 Risk Management Principles and Guidelines

This information sheet assumes a better practice environment where a risk framework has already been developed. The structure of this information sheet includes a series of better practice elements for each of the steps of the risk management process. Individuals using this information sheet should consider all elements within each step, then based upon the scale or complexity of the activity, make informed decisions as to what elements are applicable.

Establishing the scope, context and criteria

This step is used to develop an understanding of the environment in which the risk management process will be undertaken. For risk management processes to be effective they need to operate in conjunction with the entity's organisational goals and objectives.

Essential elements

Work within the existing risk management framework - It is important to identify all available elements of the risk management framework. These can include risk registers/templates, risk matrix, likelihood and consequence criteria, policies and appetite/tolerance statements. These artefacts are important to have at hand as they provide structure and guidance in evaluating the significance of a risk and on how the organisation wants the risk management process to be documented.

Identify objectives - Having clearly articulated objectives will also aid in the development of objective centred risks, which aid in understanding what really matters to the achievement of the activity and as such, what needs to go right above all else. A good place to start when identifying objectives is the entity's corporate plan.

Identify stakeholders - It is important that you identify and document all relevant stakeholders who will be able to contribute an informed view throughout the risk assessment process, noting that this list needs to be proportionate to the activity being undertaken.

Internal context - In the context of a risk assessment process, the internal context refers to the internal environment in which the entity/process functions and seeks to achieve its objectives. When doing this, consider factors such as:

- objectives and strategies in place to achieve goals
- governance, structure, roles and accountabilities
- capability of people, systems and processes
- changes to processes or compliance obligations
- the risk tolerance and appetite of the organisation
- the entity's corporate plan
- physical and technological infrastructure and maintenance arrangements
- locations of business sites and other operations
- details of internal stakeholders
- the prevailing culture and workforce morale.

External context - When undertaking a risk assessment within an entity, the external context refers to the environment in which the entity operates and seeks to achieve its objectives. The following inputs should be considered as they relate to social, cultural, political, legal, regulatory, financial, technological, economic and environmental factors, including:

- Strengths, weaknesses, opportunities and threats
- Relationships with, perceptions and values of, external stakeholders such as clients

- Environment - business, social, regulatory, cultural, competitive, financial and political situation.
- The complexity of networks and dependencies when managing risk

Risk management context - When undertaking a risk assessment within an entity it is important to identify, understand and use the documents, processes, policies, reporting mechanisms and templates that have been created to aid in the management of risk within the entity. Understanding the risk reporting frameworks is also important to ensure that the risks discovered and managed by the current risk process are incorporated into the broader risk management activities of the entity.

Risk identification

The risk identification process is most effective when key stakeholders are involved in structured brainstorming workshops. Discussions in these workshops should be supported by the outputs from the prior step; establishing the context.

Essential elements

Sources or causes of risk - For each risk identified ensure that its source or cause is well understood and documented. Be aware of risk arising from tasks/actions that seem harmless or well-controlled. Often it is the risks that an entity thinks it is managing really well that can have the most detrimental impact upon the entity when realised because no-one thought it could happen.

Identify consequences - Understanding the consequences that are realistic allows for an appropriate categorisation of severity. While personal injury is a possible result of many activities that we undertake, it is not helpful to identify that as a consequence in every circumstance due to how unlikely it is for that level of harm to occur.

Categorising risk - When undertaking risk assessments it is important to think about how risks are classified and whether any logical alignment exists across risks and risk groupings. Risk categories are high level descriptive terms to aid in the identification and analysis of risks. These help to communicate the areas of risk that are important to the organisation. For example, risks that arise from the financial management of the entity, or regulatory/policy compliance. The risk framework already established by the entity should contain a breakdown of the risk categories and their respective consequence criteria descriptions.

Risk identification scope - There is no point doing an assessment if it has no benefit to the achievement of outcomes or the success of the entity. Take time to identify what purpose the risk assessment serves in the reduction of uncertainty and the enhanced delivery of outcomes. This may result in a different focus for each activity. For example, a new internal process that does not affect client service delivery will only require the risk assessment to take into account risks that are within the organisation.

Structured vs informal risk process - It is important that the risk assessor is aware of how structured the risk assessment needs to be. It is inefficient to use hours of time to document and undertake an in-depth risk assessment for something very small and simple. You should consider how much detail is required, and how complex the analysis should be. For example, for a small procurement, an exhaustive risk assessment that takes into account the entirety of the entity environment in minute detail is not efficient nor is it likely to be effective. Risk management is by nature something that is aimed at providing helpful and insightful information that aids in the efficient and effective running of an organisation.

Better practice elements

Include all risks – even those that cannot be controlled - This can include shared risks that are controlled by contractors or subsidiary organisations. It is important that you are aware of any shared risks, although you cannot actively manage them, you can confirm that the other organisation is managing the risk well and be an active stakeholder in their risk management process.

Other sources of risk may be completely outside of any person’s/entity’s control including natural disasters and large destructive events. Whilst you may not be able to do anything to stop the event from happening, you can put things in place that will aid in the quick recovery from such an event. This forms a very important part of business continuity.

Involve those with appropriate knowledge in the identification process - There will be individuals and teams within your entity that will be aware of potential risks that would never occur to you. It is important that you consult as widely as practical and relevant to ensure that you do not miss anything in the identification stage as it will not be analysed in the following steps.

Considering cascading risks and 'knock-on effects' - It is important to recognise that small seemingly insignificant risks or events, once combined, can have far greater effects. Similarly, it is important to consider how many of your risks are likely to occur at the same time due to causal factors and their nature. Again, broad consultation will aid in the identification of these knock-on/cumulative effects.

Considering the cumulative effects of many risks - Consider the manner in which risks managed within business units such as branches or groups can have greater effects than anticipated should they escalate. An example: should a division that takes care of system maintenance identify the risk of falling behind schedule, the risk consequence for them could be as minor as not achieving KPIs, however for the rest of the business, if it were a key system to fail, delivery of core services may not be delivered or in extreme cases lives may be jeopardised. As such, maintenance of certain systems may become an organisational risk due to its cumulative effect.

Emerging and future risk – how far ahead do you look - When performing a risk assessment it is important to note there is a difference between current, emerging and future risk, and the risk assessor should ensure that risk identification considers all three time-frames. The nature of the organisation and environment will dictate how far ahead and how often future risks should be considered.

- Current risks are those risks that are visible and realisable in the current timeframe. They are the traditional focus of many risk assessments as they are the threats that are being managed actively right now.
- Emerging risks are those risks that are just on the horizon, they do not have the ability to directly affect the organisation right now. They need to be tracked and regularly reviewed to understand if they are transitioning into current risks and need treatment.
- Future risks are those risks that are further into the future. Their shape, scale and speed of onset are typically unknown, but by not identifying these risks there could be a future impact upon the organisation or activity.

How often should risk identification be undertaken? - The frequency of the risk identification process is largely defined by how rapidly the organisation's environment is changing. In an environment where the risks are stable and unchanging year on year, annual risk identification would be sufficient to keep abreast of emerging risks that may be on the horizon.

However, in an environment where the risk landscape is constantly changing it is important to be constantly scanning for risks that may not have been present before, but are now

directly threatening the ongoing viability of the organisation if they are realised. In the same manner, an organisation in a changing environment may need to continually review their risk register for risks that are no longer relevant.

The difference between strategic risk and enterprise risk means that it is usually sensible to look at their identification in different timeframes. Enterprise risks are those very important to the entire organisation and typically do not change rapidly, and as such, regular review is sufficient to identify any new enterprise risks that might arise. In contrast, strategic risks are directly related to the strategic objectives of the organisation and as such need to be aligned to the strategic planning cycle on a continuous basis. In either of these circumstances it is important to be mindful of events, inventions, innovations and circumstances that can unexpectedly alter the strategic environment and as such revisit the organisational strategy and its strategic risks assessment if necessary.

Opportunity vs threat, should the risk identification process look for opportunity as well? - While risk management has traditionally been seen to focus on managing negative impacts that might affect the organisations ability to achieve its objectives, it is also important to consider uncertainty which may present opportunities.

To consider risk as the effect of uncertainty upon objectives leaves a practitioner with the freedom to consider risk as both positive and negative. Uncertainty can lead to many varied outcomes, just as controls and mitigation strategies are utilised to try and limit the likelihood of a risk being realised; activities can be put into place to help encourage an opportunity to realise for the organisation and as such improve the overall effectiveness of the organisation.

Risk analysis

There is an important difference between risk analysis and risk evaluation. Risk analysis is focused on understanding the identified risks as best as possible. Whereas risk evaluation seeks to understand which risks are more important to an entity.
While risk analysis might indicate that a risk is high or low, risk evaluation determines which high risk should be treated first. Due to the limited nature of resources, risk evaluation is necessary to enable the most logical prioritisation of treatment actions.

An understanding of the risks impacting an organisation and its objectives is not the full picture. It is important to understand the likelihood of those risks, the consequences if they are realised and what controls are already in place to help minimise them.

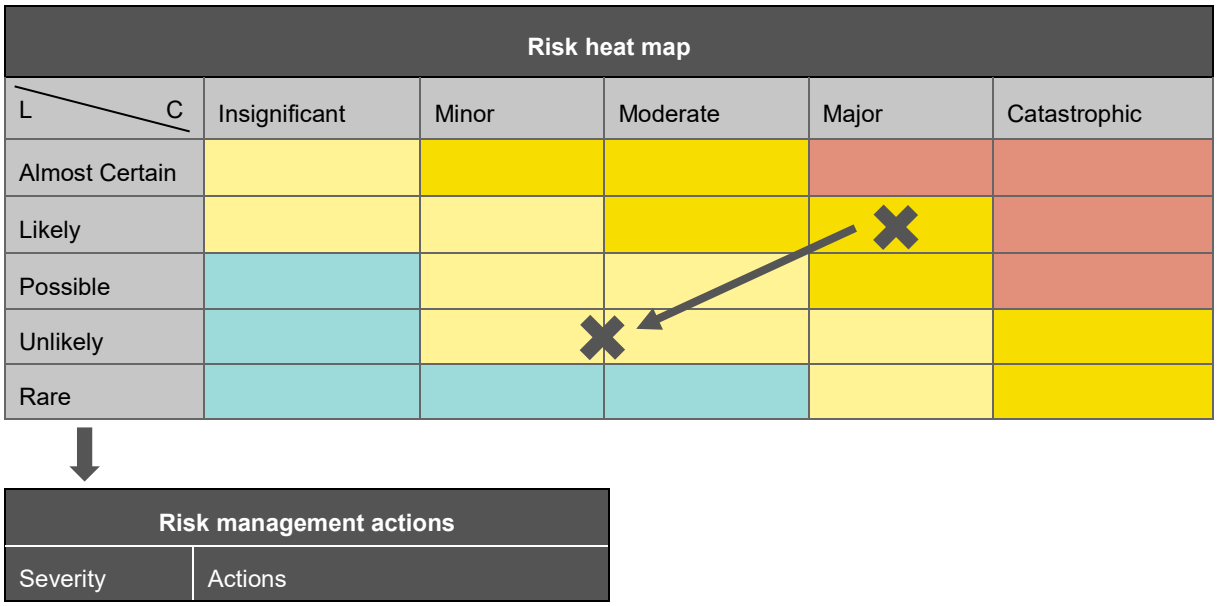
Essential elements

Likelihood - Likelihood is an assessment, based upon information available and past experience, of how probable it is for the risk event to be realised. It can range from not likely to certain. Likelihood criteria need to be calibrated to suit the organisation and its needs. This is another step in the process where reviewing the organisations risk framework will provide the appropriate likelihood descriptors and ratings that are meaningful.

Consequence - Consequence is an assessment, based upon the information available and past experience of the impact of a risk event being realised. This is generally described in terms of harm to individuals from minor to death, cost to the organisation from minimal to threatening the financially viability of ongoing operation and in terms of reputational damage. It is important that consequence criteria reflect meaningful impacts that are relevant to the organisation.

Risk severity - Risk severity is the calculation based upon the likelihood and consequence rating of the risk, generally through the use of a risk matrix, that rates the risk as low, moderate, high or extreme. Using a simple heat map to calculate risk severity

A heat map or risk matrix is a two axis matrix that tracks likelihood from lowest to greatest on one axis and consequence, from lowest to greatest on the other. Once a risk has been analysed and a consequence and likelihood rating has been given to it, a risk matrix or heat map can be used to determine the overall rating of the risk. The matrix should be developed in line with the organisations appetite and tolerance for risk. It is vital that an organisation's heat map is calibrated properly otherwise risks will be incorrectly rated for the environment and objectives of the organisation. As such, too much effort will be wasted on risks that are incorrectly identified as too high or insufficient effort will be applied to risks incorrectly rated as too low.



Extreme risk	• – • – • –
High risk	Director General attention
Moderate risk	Specific management responsibility
Low risk	• – • – • –

Inherent risk, residual risk and the effect of controls

- Inherent Risk is the level of risk to the organisation when no action has been taken to mitigate or reduce the risk. Simply put it is the risk before any treatments or controls are put in place.
- Residual Risk is the level of risk to the organisation that remains after controls have been put in place.
- Treatments are proposed actions that will further modify the risk in a way to reduce either its likelihood or its consequence, sometimes both.
- Controls are existing actions that are undertaken to modify the risk. These actions directly seek to reduce the likelihood or consequence of the risk. They are usually ongoing in nature and can involve management oversight, weekly or monthly checks, maintenance of infrastructure, training etc.

It is important to ensure the risk analysis undertaken is comparable with the magnitude of the risk being assessed. A minor risk to begin with does not need an extensive analysis, however it is important to understand, through consultation and research, that some risks that appear to be insignificant, can in fact have significant impacts in the right circumstances.

Considering interdependence – how risks can affect each other and become more severe - An important part of risk analysis is looking at the interdependence between risks. It is very rare that only one risk will be realised at a time. The greatest amount of pain or damage is caused when multiple risks are realised at the same time. Practitioners should be mindful of risks that are related to one another and as such will most likely eventuate at the same point in time. Careful examination is needed to ensure that the treatments and controls in place are sufficient to minimise or mitigate those risks as a whole.

Better practice elements

Control effectiveness - There are two aspects of control effectiveness; the design effectiveness and the operating effectiveness. If a control is not designed to adequately address the risk, then the operationalisation of it will also be ineffective. On the flip side, the control may be well designed but may not be effective when used to mitigate or treat a risk. An example of this is a well-documented process or policy. If this process or policy is not adhered to, the operating effectiveness of the control becomes compromised.

Value of considering speed of onset - Some risks are easier to identify as they begin to take shape over days, weeks, months or even years and there is value in recognising the aspect of speed of onset when analysing risks. The likelihood of an event occurring and its consequences being realised may result in an impact that is slow to be realised, and there may be instances where an observant organisation has ample time to react and as such mitigate the risk before it is realised. It is in these circumstances that considering the speed of onset can be very helpful in prioritising not only actions against risks, but also creating surveillance schedules to appropriately monitor the emergence of slower onset risks.

On the other hand there are risks that can be realised in an instant with no warning. These risks can pose a far greater threat to the organisation purely due to the possibility of the risk being realised at any moment. As such, these risks require greater attention and stronger controls when compared to an equally sever risk that has a slower speed of onset.

Quantitative vs qualitative analysis - Whilst some risks have never happened before and therefore do not have previous data, others are present in many organisations and are realised on a regular basis. These risks can be analysed using past data which may provide a more accurate likelihood of the risk being realised and consequence being calculated. Where hard data is not available to support the analysis of a risk, discussions or interviews with key stakeholders, news articles, or current happenings in the external environment may assist.

When considering quantitative and qualitative data for use in the analysis of a risk, it is important to determine the availability of data sources and the integrity of that available data. Consideration should also be given to the nature of the environment in which your entity operates, the size and complexity of your entity and the structure and reliability of your processes, technology and your people.

Risk evaluation

Risk evaluation determines the tolerability of each risk. Tolerability is different from severity. Tolerability assists to determine which risks need treatment and the relative priority. This is achieved by comparing the risk severity established in the risk analysis step with the risk criteria found in the likelihood and consequence criteria already defined.

At its simplest, an entity might decide that risks above a certain severity are unacceptable, and risks below this are tolerable. More sophisticated approaches might assign risk

acceptance delegations for risks of increasing severity to officials of different levels of seniority.

Carrying the right level of risk – not all risk is bad - Risk is not inherently a bad thing and it is important to understand that every entity must carry some level of risk in order to achieve its objectives. Risk evaluation aids an entity to understand if they are carrying the right amount of risk, thereby helping decision makers know if there are areas they could potentially take more risk in, and areas where they are carrying too much, and need to reduce.

The concept of risk appetite - As noted above, an entity cannot function if it carries no risk and it is generally accepted that in order to operate, entities will inevitably be exposed to risk. Because of this, it is important for those in charge of an organisation to be mindful of how much risk an organisation is comfortable with being exposed to. This appetite for risk should be articulated within the organisations risk appetite statement and should provide details of when the entity is willing to accept higher levels of risk, under what circumstances, and what level of control and monitoring is required.

Decisions on tolerability should also be made after considering the broader context of the risk including the impact of the risk upon entities outside of the organisation. Treatment decisions must also be made in accordance with financial, legal, regulatory, reputation, people and other requirements. Ultimately though, the considered and informed acceptance of risk supports decision making and is essential to entity performance including the achievement of objectives.

Why is it important? - Organisation resources are always limited. As such, decisions need to be made as to which identified risks are the most detrimental to the organisation's objectives and operations; this allows the treatment to be prioritised.

Given all organisations must undertake their business with finite resources, the highest priority should be given to the risks that are the least tolerable. Only by comparing risks against each other, in light of the appetite and tolerance for risk in the organisation, can a practitioner provide advice as to which risks are the highest priorities to manage.

Risk treatment

Risk treatment is a cyclical process where individual risk treatments (or combinations of treatments) are assessed to determine if they are adequate to bring the residual risk levels to a tolerable or appropriate level. If not, then new risk treatments are generated and assessed until a satisfactory level of residual risk is achieved.

Risk treatment must be tailored to the requirements and capabilities of the entity and can include strategies such as:

- Avoiding the risk entirely by not undertaking the activity
- Removing a source or cause of the risk

- Sharing the risk with other parties
- Retaining the risk by informed decision
- Taking more risk to achieve certain objectives or opportunities
- Changing the likelihood and/or consequence of the risk through modifying controls in place.

Essential elements

Selecting the most appropriate treatment requires balancing the cost and effort of implementation against the benefits derived from additional risk mitigation. In some cases, further treatment may be unachievable or unaffordable and the residual risk may need to be accepted and communicated. Entities should also consider how external stakeholders can provide support when developing treatment options or if treatments can be implemented collaboratively.

Cyclical risk treatment process

1 - Assess a risk treatment

Putting in place a risk treatment is not enough to say that the risk is now managed. It is important to assess how the treatment will modify the risk, and if it is adequately aiding in the management of the risk.

2 - Assess residual risk levels against tolerability

It is important that the risk treatment process is not done in isolation. Risk treatments need to be linked to the appetite and tolerances of the organisation.

An inadequate treatment that does not reduce the risk to an acceptable level needs review or further treatments implemented in unison to achieve the target level. In the same way, a treatment that reduces a risk too much may be wasting limited resources. A clear understanding of what the target risk level is, defined by the organisations appetite and tolerance, is key to applying treatments suited to not only the risk, but the organisation as a whole.

3 - If not tolerable, generate new risk treatment

Monitoring treatments - The risk landscape is not static; risks can change and develop new characteristics that may need additional treatments. To help manage this, regular reviews of treatments, controls and their effectiveness needs to be undertaken.

It is also important to note that on occasion risk treatments and controls can give rise to more risks that will need to be managed.

Stakeholder perceptions of treatments - Some treatments or controls may be very effective in mitigating a risk, yet they may also be unpalatable to stakeholders. Practitioners should remain aware of stakeholder perceptions of risk treatments and controls to ensure

that the organisation does not undertake an activity that is going to severely harm its relationship with its stakeholders.

Treatment Plans - Treatment plans are typically used for two purposes; as a basis to prioritise risk as part of the Evaluation stage, and, to document how the identified risk will be treated. They need to be well documented, clearly defining what tasks needs to be done, by whom and for what purpose. Things to include in a treatment plan are:

- Reason for selecting treatment options, including expected benefits
- Those who are accountable for approving and implementing
- Proposed actions
- Resource requirements
- Performance measures, and reporting and monitoring requirements
- Timing and schedule.

A treatment plan (schedule) can be as simple as a single page outline of actions to be undertaken, by certain dates. It can also be as complex as a full suite of documents that very clearly detail each treatment that must be implemented, with responsible authorities, due dates, review cycles and intended quantifiable outcomes. It is important that the treatment plan is suited to the needs of the organisation and the risks being managed.

Balancing cost, effort and benefits derived - Due to the fact that organisations have to operate on finite resources, treatments must balance the cost of implementation, the effort to put in place and maintain with the benefits derived. It is important that the benefits gained match or are greater than the energy and resources expended to achieve them.

Considering combination of treatment options vs individual treatments - For some risks a simple treatment or control will be sufficient to reduce the risk down to the target level. However, for other risks this is not the case. In some circumstances a single treatment may be too expensive or not reliable enough to bring the risk into acceptable levels. In these circumstances a combination of treatments and controls may be more cost effective and provide a greater level of reliability.

In some circumstances, either due to cost, complexity or resources available to manage a risk, it may be appropriate to engage with stakeholders to manage the risk in part or wholly for the organisation.

Collaborative approaches to developing joint-treatments for shared risks - Many risks affect multiple parts of a large organisation or even multiple organisations within a sector; in these circumstances it can be valuable to collaboratively manage the shared risk. As such, each entity can implement complementary controls and treatments to cover the gaps and inadequacies of others, in a way that manages risk as a whole and keeps costs at an acceptable level.

Monitoring and communication between the entities is vital to ensuring that vulnerabilities don’t form from a member not managing their share of the risk adequately.

Communication and consultation

Communication and consultation is an essential attribute of good risk management and is important at each step of the risk management process. Communicating risk information with stakeholders maintains confidence and trust and develops a common understanding of the entity's risks.

Formal risk reporting is only one form of risk communication. Good risk communication should:

- Encourage stakeholder engagement and accountability
- Maximise the information obtained to reduce uncertainty
- Meet the reporting and assurance needs of stakeholders
- Ensure that relevant expertise is drawn upon to inform each step of the process
- Inform other entity processes such as corporate planning and resource allocation.

Different stakeholders will have different communication needs and expectations. Good risk communication is tailored to these requirements.

The development of a communication plan, may aid in the communication of risk. The purpose of this plan is to ensure that the right information is communicated to the right people at the right time. It may include information such as the entity's attitude and approach to risk management, the risk profile, and specifics around control responsibilities and actions.

Risk communication encourages transparency of risk, leading to a more risk-aware organisation and a positive risk culture.

Monitoring and review

Monitoring and review is integral to successful risk management and should be a pre-planned and deliberate part of the process. Responsibilities for monitoring and review should be clearly defined and seen as a key management responsibility.

Key objectives of risk monitoring and review include:

- Detecting changes in the internal and external environment, including evolving entity objectives and strategies
- Identifying new or emerging risks
- Ensuring the continued effectiveness and relevance of controls and the implementation of treatment programs
- Obtaining further information to improve the understanding and management of already identified risks

- Analysing and learning lessons from events, including near-misses, successes and failures.

Monitoring and review can be periodic and based upon trigger events or changing circumstances. The frequency of the review process should be commensurate with the rate at which the entity and its operating environment is changing.

Recording and reporting

The results and observations from the risk management process are most useful when well documented and shared. They may be included in formal risk reports, and published internally and externally as appropriate and should also be used as an input to reviews of the whole risk management framework. Reporting is an integral part of the organisation's governance and should enhance the quality of dialogue with stakeholders and support top management and oversight bodies in meeting their responsibilities

Key objectives of recording and reporting include:

- Communicating risk management activities and outcomes
- Inform corporate planning and decision making
- Improve risk management activities
- Assist interaction with stakeholders

As part of the documenting the risk management process, your risk report should include:

- How you defined the environmental context you were operating in (for example undertaking an analysis of the political, environmental, social, technological, legal, economical and internal organisational conditions)
- How you undertook your risk assessment – including identification of controls and treatments (for example through a facilitated workshop)
- When you will implement your treatments (for example treatments will be triggered as per the guidance of your risk management framework or if the risk goes beyond the tolerance set by the risk owner that it has been endorsed by your Deputy Secretary)
- Who you communicated and consulted with throughout the process (such as key internal and external stakeholders who can effect or be effected by your work)
- Your monitoring and review process and schedule.

A risk report can be a tool to provide evidence that the risk assessment process and actions arising from it were thought through in a structured process before being actioned.

Contact

If you have any questions or feedback in relation to this information sheet please contact Comcover Member Services at comcover@comcover.com.au.

Use of this information sheet

Comcover's series of Risk Management Information Sheets are designed to be used as learning resources and are not mandatory.

It is important that entities develop risk management frameworks and systems that are tailored to the needs of their entity. Entities may choose to adapt some or all of the concepts contained in this information sheet to suit their specific needs or use alternative methodologies.