Comcover Information Sheet

Framework

Maintaining an Entity's Risk Profile

Purpose

This information sheet is intended to assist Commonwealth officials at the Specialist level understand:

- what a risk profile is and how they can be presented,
- how a risk profile can be used to support decision making, and
- practical steps for developing, maintaining and reviewing a risk profile.

At a glance

A risk profile is a description of any set of risks. The set of risks can contain those that relate to the whole entity, part of the entity or as otherwise defined.

An entity's risk profile can contain risks of different natures. Some of these may be managed at an enterprise level and represent the most significant risks exposures of the entity, others will be managed within business units and represent more focused concerns.

What information can a risk profile provide?

Risk profiles can be represented in different ways and can be used to highlight different messages to different audiences.[1]

Examples of some of the issues a risk profile can communicate include:

- The overall level of risk being carried by the entity.
- How the entity's current risk exposure compares to its appetite for risk.
- Themes, patterns or common issues amongst the entity's risks.
- Areas of shared risk or interdependency.
- Warning of emerging or worsening risk exposures.
- Detail on the nature of individual risks.

[1] Appendix A provides examples of how risk profiles can be represented.

How can a risk profile be presented?

The underlying data for an entity's risk profile is commonly contained in one or more risk registers. Typically, each risk register contains information in a spreadsheet or database format. For each risk, this might include the risk event, its category, the inherent risk rating, sources or causal factors, links to risks in other registers, controls and control effectiveness rating, and residual risk rating. Each entity will present this differently though in a format that suits them. An illustrative example of a simple risk register is provided at Appendix A.

As a typical risk register contains a lot of detail, it is not always the best way of presenting risk information to senior decision makers. A risk profile can be an effective way of summarising the information held in the entity's risk registers in an easy to understand format.

Consider the audience and their information needs when portraying the risk profile. Four examples of different risk profile representations are provided at Appendix A. They include a simple risk register format, a 'heat map' or risk severity matrix[2], a graph of inherent risk against the effectiveness of current controls, and a comparison of risk severity against risk tolerance.

Who is responsible for maintaining a risk profile?

Ultimately, the accountable authority is responsible for ensuring the appropriate management of an entity's risk profile. In practice, the manager/s of the entity's risk registers, and therefore the profile, will vary depending on the size, nature and complexity of the entity. The table below highlights how risk profile maintenance can be devolved, centralised or managed in a hybrid model.

Devolved	**Centralised**	**Hybrid**
In a devolved model, business units maintain their own risk profiles and communicate risk information independently to the executive committee. Very little centralised support to risk profile development, analysis or maintenance is provided. A devolved model can be beneficial where business units are managed with a high degree of autonomy. It provides for flexibility and suits a model of decentralised business decision making.	In a centralised model, risk is identified and assessed and then provided to a centralised function who maintain risk profiles across the entity. Risk recording, profile maintenance and analysis, and control monitoring is centrally coordinated. The benefits of centralised model includes economies of scale, minimal duplication of work and well-defined reporting lines. It also promotes consistency and suits entities where most decision making is made at the enterprise level.	In a hybrid model risks are identified, assessed and managed to in all areas of the entity. However a central risk function supports the maintenance of the devolved risk profiles and coordinates reporting and analysis information as well. The Hybrid model suits where business units are required to be accountable for managing their risks and where decision making requires a degree of collaboration

[2] This representation is often referred to as a 'heat map' as the severity of the risk is traditionally illustrated by colour shading with 'hot' red colours indicating severe risks, and 'cool' green colours indicating less severe risks.

What are the benefits of using a risk profile?

Better informed decision making and corporate planning

A key purpose of a risk profile is to support effective decision making in circumstances of uncertainty.

By clearly highlighting where key risk exposures exist, senior decision makers can work to manage these and avoid action which would drive the risk outside of acceptable tolerances.

Improved ability to anticipate change, emerging risk and disruption to operations

A risk profile can support the consideration of emerging and future risk as well as current exposures so that contingency plans can be developed where required.

A disciplined approach to risk profile maintenance includes an ongoing process to identify new or emerging risks and analyse the threats and opportunities they may represent. This process helps the entity to:

- understand the likely effectiveness of existing strategies and controls in mitigating emerging risk and optimising opportunity,
- understand how new risk changes the overall exposure of the entity,
- understand the impact that the changed risk profile could have on stakeholders and shared risks, and
- anticipate change and disruption to operations.

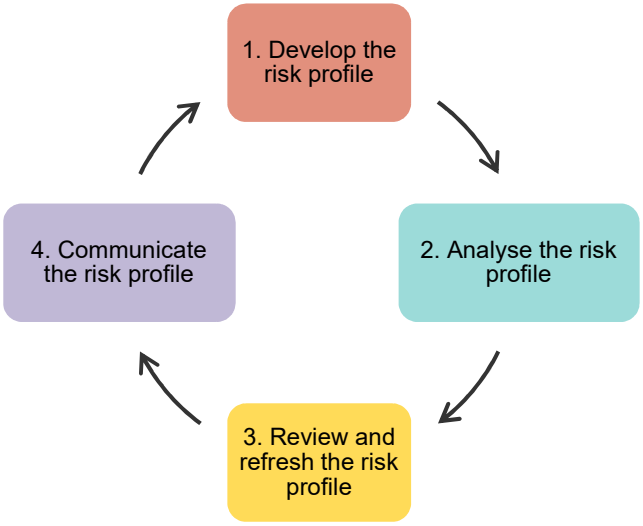
Understanding risk exposure compared to risk appetite

A good representation of an entity's risk profile will support senior officials to understand whether the entity is holding too much, too little, or just enough risk.

Where an entity has a well-defined risk appetite, this can be represented within the risk profile. The risk profile can be used to clearly highlight where activities, programs or business units are operating outside defined risk tolerance thresholds.

A practical approach to developing, maintaining and improving a risk profile

The following is one approach to developing, analysing, maintaining and communicating a risk profile. The actual process used may be tailored to the specific needs of each entity or circumstance.



Step 1 – Develop the risk profile

A first step is to develop the risk profile by conducting a risk assessment and capture the outcome in a risk register. Depending on the size of the entity, its risk profile may be developed from one or many individual risk assessments.

When developing the risk profile:

- assess risk with both a short and long-term focus (his enables the subsequent risk profile to inform both immediate action and longer term planning),
- seek input from stakeholders and relevant subject matter experts who best understand the risks, and
- develop the risk profile in accordance with the relevant risk management framework and ensure consistent and correct use of risk terminology and categories.

Although it differs between entities, the corporate planning process will commonly link the entity's corporate and business unit plans to its objectives. These objectives form a crucial starting point for any risk assessment in the entity, and a key focus of the entity risk profile is to manage the uncertainty around their achievement.

Step 2 – Analyse the risk profile for common themes and systemic issues

Just as individual risks are analysed to fully understand them, the risk profile can be analysed to identify key,common or systemic issues between and amongst the risks. Understanding these can focus attention on where the most effective change can be made.

Examples of patterns, themes and issues to look for include:

- patterns in the difference between inherent vs residual risk (the extent and consistency of difference will give an indication of the effectiveness of the entity's control framework),
- common causal factors, where a small number of contributing issues are relevant to a larger number of risks (these may suggest priority opportunities for treatment),
- linkages between risks in different profiles (this can help understand interdependencies, relationships and the opportunity for cascading failures), and
- concentrations of severe risk in certain categories may indicate areas of particular vulnerability for review (for example, if an otherwise robust entity is managing a number of severe risks within one category it may indicate attention needs to be paid to this area).

Step 3 – Continuous review and refresh

Any risk profile needs continual maintenance. In part, this determines if there have been any changes to the risk profile caused by changes to the internal or external context. Reviewing the risk profile can assist in ensuring that:

- assumptions about risks remain valid and the external and internal context in which the risks were assessed remain valid,
- results of risk assessment are in line with actual experience,
- risk controls are being maintained and assured, and that proposed treatments are being implemented as required, and
- assumptions around the interrelationships and linkages between risks at all levels at the entity and the impact of change in one risk on another, remains valid.

The monitoring and reporting cycles of corporate plans and risk profiles can be aligned to create synergies between the two activities. The monitoring and review process needs to keep pace with changing priorities and the refresh of the corporate plan is a good opportunity to refresh the relevant risk profiles in their entirety.

Practical strategies that can be used to guide the review of an entity's risk profile include:

- Having a relevant risk owner or steward present an analysis of a small number of risks with a focus on key changes or concerns. Over time, this will result in a rolling program of review of the risk profile.
- Avoid the practice of reviewing every risk in a risk profile in a single meeting or session. Doing so can lead to compliance behaviours and skipping over the risks that require the most attention.
- Periodically recreate the risk profile from a 'clean sheet'. Occasionally starting from scratch and performing afresh risk assessment and then reconciling the results with the

existing profile is a great way to ensure you don't become fixated on simply refining existing risks.

- Establish escalation mechanisms to ensure that risks in the entity risk profile are being managed at the right level.
- Ensure those responsible for designing or implementing new policies or programs first review relevant elements of the risk profile to ensure that they understand whether risks will be created or modified and that control strategies remain appropriate and effective.
- Consider risk monitoring information already available such as audit reports, quality assurance activities, and the results of key performance indicators.

Step 4 – Communicate the risk profile

Ensure that the risk profile is communicated to the right people at the right time in an appropriate format. Some considerations when communicating the risk profile include:

- seeking feedback from executive reviewers and stakeholders on how often and to whom risks are to be reported,
- establishing well understood risk escalation and aggregation protocols so that unacceptable risks can be quickly conveyed to the appropriate level of management and that the nature of the risk is clear,
- tailoring the presentation of the risk profile to its audience and consider their risk management maturity, and
- using colour to highlight key issues and areas of concern, or focus the audience's attention on the risks or concerns that most warrant discussion.

For further information on risk communication refer to the Comcover Information Sheet Communicating Risk.

Appendix A – Examples of risk profile representations[3]

Example 1. Traditional Risk Register

Although they vary in scale and complexity, a simple risk register may typically contain the following elements for each risk:

- risk ID or unique identifier,
- description of the risk – its cause, the risk event, and key outcome should it be realised,
- a risk category or group or family,
- sources or causal factors relevant to the risk,
- the likelihood of the risk occurring,
- the potential consequence should the risk be realised,
- control measures currently in place and an assessment of their effectiveness,
- an assessment of how the risk is changing or trending and how quickly it could be realised,
- an assessment of risk tolerability, or how the risk compares to relevant elements of the entity's risk appetite,
- treatments (proposed controls) to be implemented to improve the management of the risk, if required, and
- owner or steward of the risk.

[3] These representations are examples only and not recommended for use in circumstances where they may not be fit for purpose.

The table below is an illustrative example of a simple risk register.

	Risk Category	Risk Description	Likelihood	Consequence	Inherent Risk Rating	Control Rating	Residual Risk
1.	Stakeholder Management	Failure to agree outcomes or maintain a healthy relationship and consult with Stakeholder X	3	4	7 S	4 E	M
2.	Legal & Regulatory Governance	Failure to comply with regulatory and statutory requirements	2.9	3.2	6.1 M	4 E	L
3.	Stakeholder Management	Significant and ongoing adverse stakeholder reaction	3.7	4.1	7.8 S	2 E	M
4.	Workplace Health & Safety	Workplace Health and Safety is compromised	3	4.5	7.5 S	3.4 E	M
5.	Environment & Sustainability	Risk of inadequate planning to avoid future significant adverse environmental impacts	2.3	4	6.3 M	1.9 IE	M
6.	Finance	Fraud or improper actions	2.9	3.1	6 L	2.4 E	L

Legend		
Inherent risk ratings	Control rating	Residual risk rating (RR)
H High risk	E Effective control environment	H High risk
S Significant risk	IE Ineffective control environment	S Significant risk
M Moderate risk	NA Not assessed	M Moderate risk
L Low risk		L Low risk

Example 2. Risk Severity Matrix or Heat Map

A risk 'heat map'[4] or risk severity matrix plots the risks in a risk profile on a matrix or graph, with the scale of consequence on one axis and likelihood on the other. Colours and banded levels are often used to highlight risks of differing severities.

An example of a simple risk profile represented as a heat map is illustrated below. Each numbered circle refers to an individual risk. The structure of the heat map and the severity levels will be defined in the entity's risk management framework and should reflect the considered risk appetite of the entity.

Residual Risk Severity					
Likelihood/ Consequence	Insignificant	Minor	Moderate	Major	Severe
Almost Certain	Medium	Medium	High	High	Extreme
Likely	Medium	Medium	Me 9	5 12 6	Extreme
Possible	Low	Me 11	Me 3	High	High
Unlikely	Low	Low	Me 4	Me 1	High
Rare	Low	Low	L 10	Me 8	7 dium 2

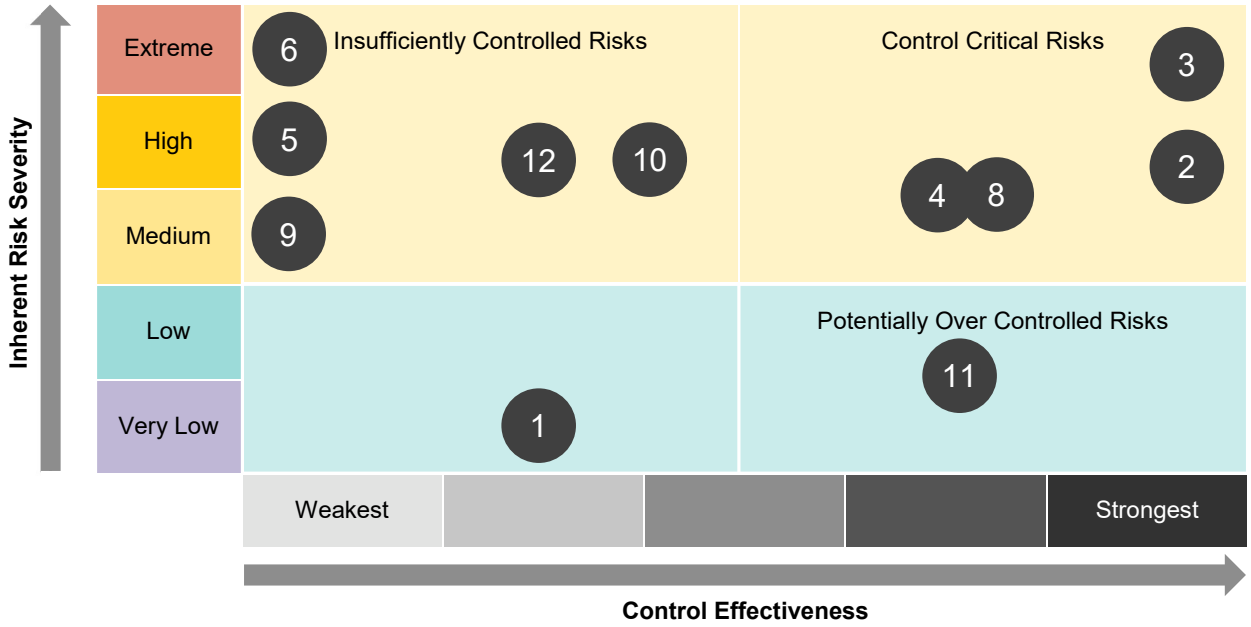
[4] This representation is often referred to as a 'heat map' as the severity of the risk is traditionally illustrated by colour shading with 'hot red colours indicating severe risks, and 'cool' green colours indicating less severe risks.

Example 3. Inherent risk severity vs control effectiveness

Other representations of a risk profile may seek to communicate a particular message, concern or pattern.

The example illustrated below plots the control effectiveness rating of the risk on one axis and the inherent risk severity on the other. Again, each numbered circle refers to a risk in the risk profile.

This particular representation shows whether risk control strategies are effective in managing the entity's risks,and where further investment may be needed. It helps differentiate those risks which are inherently low and those which are only low because of a high degree of control effectiveness (control critical risks).



Control critical risks - are inherently severe, but currently well controlled. They may represent a low level of residual risk but only because of the effectiveness of current controls. These risks require active monitoring and management and an assurance strategy to ensure the risks do not increase in severity.

Insufficiently controlled risks – are inherently severe and are assessed as being inadequately controlled. They may represent high residual risks. Insufficiently controlled risks likely require additional treatment.

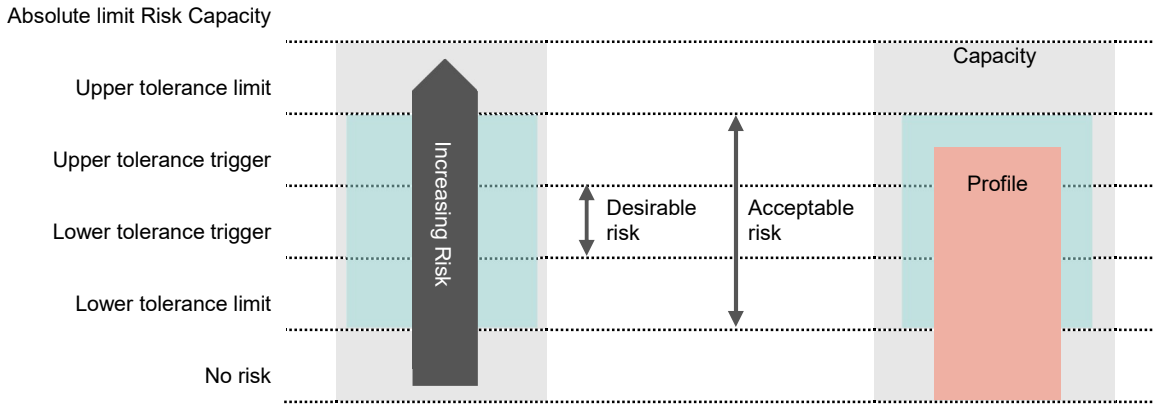
Inherently low risks - require active monitoring to ensure that any changes in the internal and external context do not make the risk more severe.

Potentially over controlled risks - are inherently mild with high levels of control. These risks need to be monitored to ensure they do not become more severe over time, but also represent potential opportunities for efficiency gains if redundant or excessive controls are found.

Example 4. Risk exposure compared to risk appetite

It can be useful to explicitly compare the level of risk exposure represented in a risk profile against the risk appetite of the entity. This helps decision makers understand if they are carrying too much, too little, or just enough risk. This can occur at an individual risk, risk category, or whole of profile level.

In the conceptual example illustrated below, the entity's risk profile (or exposure) represented in red is outside the most desirable risk tolerance band. Action may need to be taken to reduce the risk, particularly if the risk assessment suggests the risk is likely to rise further.[5]



The manner in which this is represented in practice will vary depending upon how the entity articulates its risk appetite and the target audience. Illustrated below is a simple table that presents a risk profile of six risks, comparing the current exposure against the risk tolerance for that category of risk. The rightmost column clearly illustrates to a senior decision maker where risk is above, below or in line with the relevant tolerance and the direction the risk needs to be driven.

[5] For further information on the concept of risk appetite see Comcover's Information Sheet Understanding Risk Appetite.

Risk	Risk Severity	Risk Category	Risk Tolerance	Required Action
Failure to agree outcomes ormaintain a healthy relationshipand consult with Stakeholder X	High	Stakeholder Management	Medium	
Failure to comply with changing privacy regulatory and statutory requirements	Medium	Legal & Regulatory Governance	Medium	
Significant and ongoing adverse stakeholder reaction to Project X	Low	Stakeholder Management	Medium	
Workplace Health and Safety is compromised at Facility X during refurbishment program	Medium	Workplace Health & Safety	Very Low	
Uncontrolled waste treatment spillat Facility X	Low	Environment & Sustainability	Low	
Smoke scrubber failure at Facility X	Medium	Environment & Sustainability	Low	

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 suittheir specific needs or use alternative methodologies.