Case Study: Defining Risk Appetite and Tolerance

Department of Employment

Audience

This information sheet is intended to assist Commonwealth officials at the following levels:

- **Specialist level:** Job role specialists who are required to design, implement and embed an entity's risk management framework.
- **Executive level:** Senior executive service officials (SES) whose role requires them to identify and determine the acceptable levels of risk that are appropriate to their agency's profile, allocate resources and lead the adoption of risk management policies, strategies and best practices.

At a glance

The Department of Employment (the Department) was finding that, despite their relatively mature risk culture, there were inconsistencies emerging in the way the Department's officers understood and assessed risk. This included cases where low level risks were being escalated to Senior Management in the same way as strategic and more complex risks. In order to provide greater clarity to officers of the Department on what constitutes acceptable risk taking, the Department completed a project to review its Risk Appetite Statement and overarching Risk Tolerance.

Outcomes of this review included:

- recalibrating risk categories to support the Department's strategic objectives
- defining risk appetite and tolerance across categories and sub categories of risk
- subsequent recalibration of the risk matrix and other elements of the risk framework to reflect the newly defined risk appetite
- a new approach to assessing risks that considered not only inherent risk, control effectiveness and residual risk, but also velocity and assessor confidence.

The following case study presents some details of the process that the Department undertook to redefine its risk appetite, as well as some lessons learned that they identified during the process.

The ten step process

A ten step process was developed for the risk appetite review which began with the identification of a reference group. This reference group participated in the first iteration of risk definition and tolerance, assisted in managing the ten step process and ensured progress was maintained. This reference group agreed the remaining nine steps to be followed, which in summary include:

1. Appoint a core reference group
2. Validate current risk categories
3. Review current risk profile
4. Build a risk appetite statement template
5. Interview senior executive and define risk appetite statement
6. Engage with SME's to build and refine risk tolerance statements
7. Senior executive review
8. Amend risk appetite and tolerance statements as required
9. Committee Validation
10. Incorporate and communicate

1 - Appoint a core reference group

The Department brought together a small core reference group of people to draft, refine, workshop, test and deliver the work. This reference group contained staff members who would write and develop most of the work as well as senior leadership to help shape direction and provide senior insights.

Key subject matter experts both internal and external to the Department were also included in the group to ensure that each category of risk was developed by those with informed views. Key factors to the success of the project was keeping this group small and selecting only those who were actively going to work together and be available to see the project through to its completion.

2 - Validate current risk categories

The Department agreed that they would define Risk Tolerance at the risk sub-category level. Consequently, the first step was to review the Department's risk categories to ensure they accurately reflected its strategic objectives.

There are two broad ways of defining risk categories, grouping risks by their source; or by their consequence. For example, "People" can be a source of risk and risks can have consequences on people. The Department used the latter to frame the defining of its risk categories and supporting sub-categories.

To validate that the right categories had been developed, the Department's senior executive were asked the following three questions:

- Are these the consequences/impacts the Department is most concerned about?
- Do they help the Department better manage its risks?
- Do they clarify peoples' thinking on risk?

Following this, five main risk categories and supporting sub-categories were developed. These sub-categories were broad enough to capture all possible risks, but specific enough to assist in understanding which risks were similar in nature. The Department chose to have sub-categories to provide richer detail in the consequence categories. The theme and number of sub-categories is a subjective topic based on the Department's risk profile.

3 - Review the current risk profile

After the review of the risk categories, the enterprise risk profile was reviewed to identify key risk themes and consider how the current profile would translate to the new categories. These themes assisted in understanding the context, priorities and sensitivities of the Department which informed subsequent discussions to define risk appetite and tolerance levels.

4 - Build a risk appetite statement template

To assist stakeholders in being able to differentiate the Department's appetite and tolerance for risk across the categories a template was developed. The Department chose a template that illustrated tolerance through the use of a tolerance scale for each sub-category of risk. Presenting this information visually enabled stakeholders to directly compare their tolerance for one sub-category of risk against another, thereby avoiding the tendency to have no or low tolerance for risk in all categories. This template evolved during the process.

Below is a simplified version of what the scales looked like.[1]

5 - Interview the Department's senior executive and define risk appetite statement

The Department's senior executive were then interviewed to firstly discuss and agree an overarching risk appetite statement for the Department and then to define the risk tolerance statements for each category of risk. While it was challenging for the senior executive to articulate appropriate levels of risk taking, a structured process was used to encourage useful debate on what constitutes desirable, acceptable and unacceptable risk.

Consideration of where the Department would invest resources to manage the categories of risks served as a good way of understanding the relative priority/tolerance of one risk category or sub category to another. Participants were asked if they had one last dollar, with which they would reduce risk, where they would spend it. The answers indicated which risks they had the least tolerance for.

We also reflected honestly on actual and historical behaviour for clues about relative tolerance, both between risk categories, and within risk categories. For example, observing actual behaviour in recent years, had the department reacted more adversely to harm to people or to reputational damage (i.e. between risk categories)? Had the department reacted more adversely to reputation risk in the international context than the domestic context (within the risk category of reputation)? This was then reflected by the use of risk tolerance scales in the template built earlier.

Other key questions asked during the consultation were:

- what types of risk are unacceptable?
- what does good risk-taking look like in our Department?
- under what circumstances do we accept risk

[1] Note – for the Department of Employment this was not used at a category level as pictured. Instead each of the five main categories has a range of tolerances underpinning them

6 - Engage with Subject Matter Experts (SMEs) to build and refine risk tolerance statements

After the initial definition of risk tolerance levels and statements, an iterative process of consultation and refining them was undertaken. This began with subject matter experts, whose input was sought regarding risks that were relevant to them. For example, the CFO was directly consulted on financial risk.

After consulting with SMEs, the Senior Executive was engaged again. This cycle of engagement continued until the risk tolerance levels and statements were sufficiently defined.

7 - Senior executive review

Once the reference group was comfortable that the risk appetite and tolerance statement articulated all the key messages and necessary content, it was shared with the senior executive for their review. Even though many of them had been consulted in the process and their views incorporated, it was important to provide a final draft to them and test if they were comfortable as a group, not just as individuals.

8 – Amend risk appetite and tolerance statements as required

Following the senior executive review, amendments were made to ensure that the appetite and tolerance statement reflected all nuances that they wanted to convey as a group going forward. This was important as the statement focuses and directs the conversation of risk into the future at both a senior level and throughout the organisation.

9 – Governance committee validation

Prior to the risk appetite and risk tolerance statements coming into effect, endorsement from the Department's Risk and Implementation Committee and the Secretary were sought. This was the final review required before implementation could take place.

10 - Incorporate and communicate

With a new risk appetite and risk tolerance statement articulated in line with the revised risk categories, the risk management framework also needed to be updated to ensure alignment and support change management and communication. The consequence and likelihood criteria for the matrix were the first artefacts revised to align with the risk appetite and tolerance. Then the risk matrix changed so that areas of the matrix that indicated high and low severity (and all gradients in between) also reflected the risk appetite and risk tolerance statements.

Finally, to further develop the Department's risk assessment capability, new scales were developed to assist in better understanding risks and their treatments including:

- a vulnerability assessment, which was designed to look at how well current controls and treatments mitigated the risk
- a velocity scale to capture how rapidly a risk may be realised and its nature
- a confidence scale to allow risk managers to look at risks through a lens of how well the risk was understood and assess the level of confidence in the assessment.

Next steps

Once an organisation has successfully articulated its appetite and tolerance for risk, this understanding needs to be embedded into the way people engage and manage risk on a day to day basis. A clearly articulated and defined appetite and tolerance is very valuable to senior management in clarifying their thinking, assisting in planning and resourcing and prioritising effort. A new risk appetite and tolerance statement needs to be operationalised within the organisation through the risk matrix and associated consequence and likelihood criteria.

As with all aspects of risk management, a key element to the success of an organisation is ongoing monitoring and review. After an organisation has gone through the processes of articulating and embedding their appetite and tolerance for risk, systems need to be put in place to ensure that it remains current to the operating environment of the organisation and the thinking of the senior executive.

The steps to embedding risk appetite and tolerance in an entity

Establish a core reference group

The process took over six months and involved a number of iterations. The Department found it invaluable to have someone senior, preferably a member of the Executive, in the group. Having a stable reference group that were constantly engaged and did not change allowed the momentum to continue. Additionally, it is important to use an expert who understands your needs without trying to push their own service model.

Don't start from scratch – build on what you have

It is important to build on existing risk culture and framework. The Department already had consequence descriptors so these were reviewed and tweaked to create new categories. They built on what we had and didn't just dismiss existing thinking and practices. This saved time, and helped stakeholders understand how their thinking was maturing.

Secure a strong senior executive sponsor

It is essential to have a senior executive sponsor to drive the change process, answer executive questions, and support senior management through the process. This allowed the team to be confident that senior management was well aware of the work.

When selecting a sponsor, look for a hands-on leader who is passionate about risk management with an awareness of the risk culture of the organisation. This ensures that the language and pitch of the risk appetite will be familiar and comfortable to senior stakeholders from the beginning.

An effective sponsor when defining risk appetite also helps avoid small 'p' politics. All risk appetite is a trade-off, there's always a further nuance that can be made or a category that can be added. Risk management by essay isn't very effective, so eventually someone will need to subjectively decide what will be included and why.

Start with a small stakeholder group and grow

Starting with a small stakeholder group and building outwards helps ensure that the product is well grounded. A risk appetite statement will never be all things to all people, and it's important to have a considered rationale for what is included and what isn't. This prevents the 'buzzword of the day' from being included just because it is currently popular.

Give stakeholders something to react to

With a new risk appetite and risk tolerance statement articulated in line with the revised risk categories, the risk management framework also needed to be updated to ensure alignment and support change management and communication. The consequence and likelihood criteria for the matrix were the first artefacts revised to align with the risk appetite and tolerance. Then the risk matrix changed so that areas of the matrix that indicated high and low severity (and all gradients in between) also reflected the risk appetite and risk tolerance statements.

Challenge senior executives

When consulting senior executives, it is important to use a facilitator who is comfortable enough with senior stakeholders and risk management to know when to stop a conversation and bring it back to the challenge at hand.

Remember that risk tolerance is relative

The Department found that when risk tolerances for certain categories were viewed in isolation, there was a tendency for stakeholders to instinctively say they had little to no tolerance. It was only when a more real-world view was taken such as 'how about compared to harm to the public' that they were able to define their 'true' tolerance.

Keep it simple

Don't add detail just for the sake of it as more detail doesn't necessarily improve understanding. The Employment risk appetite statement uses a simple visual slider to discuss relative tolerance. The 'units' on this slider aren't defined because they don't have to be, they're only important relative to each other.

Drill down until it hurts

If you're using consequence categories, drill down until it hurts. When trying to determine your risk consequence categories, frame any conversation by emphasising that all negative risks aren't equal. Instead try asking the 'so what' question until you're satisfied with the underlying answer. For example: do we care about a hypothetical release of confidential information just because? Or is it because we've breached the law? Or is it because we've harmed someone?

Contact

If you have any questions or feedback in relation to this information sheet please contact Comcover 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 organisation. 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.