8

Appetite for business

Does it matter?

A great deal of information about risk appetite statements is available to risk professionals. Some has been generated by regulators, who publish better practice guidelines or prescribe specific requirements for risk appetite statements; more is produced by industry associations and service firms. Maybe you have had some success with these sources, maybe not. I have helped many organisations with them, so let me give you my thoughts on them and whether they really matter.

> No one wraps themselves up in cotton wool and hides away from the world to live life absolutely risk-free.

First and foremost, we all have an appetite for risk. No one wraps themselves up in cotton wool and hides away from the world to live life absolutely risk-free. Second, appetite for different types of risk varies from person to person. Some of us will not risk our health by smoking cigarettes but will jump at the chance to sky dive; others smoke but would never dare to sky dive. Third, every day we take our individual appetite for risk to work and apply it to our decision making. Staff need to understand the organisation's appetite for risk-taking and that it overrides their personal beliefs. Lastly, a risk appetite statement should be firmly embedded in your organisation's strategy. It's all about understanding the opportunities ahead and the potential risks in pursuing them, and about making clear decisions on which ones to pursue and how aggressively. Thankfully, the need to link risk appetite and strategy is clearly articulated in the most recent COSO (Committee of Sponsoring Organizations of the Treadway Commission) guidance on risk appetite.[16]

A risk appetite statement should be firmly embedded in your organisation's strategy.

To be honest, when I first heard about the drive for documented risk appetite statements, I thought it was being dreamed up by consultants to make money. What I came to realise was that I understood the risk appetite of an executive team because I was facilitating risk workshops for them. It was all the staff not in the room with us that were having a problem understanding it.

While a regulator's requirement or a desire for best practice have been drivers of some organisations whose risk appetites I have helped document, the main reason people have come to me is the best reason: because middle management is unclear on the board's or the executive's appetite for risk *in fulfilment of the organisation's strategy*, and the board and/or executive want help articulating it as succinctly and effectively as possible.

However, your board or executive team may simply be ticking a box with risk appetite. If that is the case, start with this. Highlight for them the problem of individuals applying their own appetite for risk and ask them this question: 'Are many people in the organisation spending time on things that are unimportant to you and not spending time on aspects of the business that are important to you?'

'Are many people in the organisation spending time on things that are unimportant to you and not spending time on aspects of the business that are important to you?'

The answer to this question is likely always to be yes. The bigger question is, to what degree? The greater the gap between their expectations and reality, the greater the benefit they would derive from driving an understanding of risk appetite deep into your organisation's DNA, resulting in staff spending more time on value-creating activities, and less on activities that are less important, or not important at all!

There's one more phenomenon you need to understand, however. It became very clear to me years ago when I was running risk champions training for a team tasked with putting workers in a high-risk and emotionally stressful environment. I was talking about the need to design policies, processes and systems to guide decision making 'so staff will make the same decision the CEO would make'. Then, from the middle of the pack of 25 in the room came, 'Bullshit! The CEO would not know shit when it comes to some of the decisions we need to make.'

> Leaders hire staff with specialist skills to get the job done.

Of course he was right. Leaders hire staff with specialist skills to get the job done. The CEO can't be a specialist in all areas. So what happens in organisations is that senior management are trying to influence decision making below them and out to the extremities of the organisation. Meanwhile those at the extremities are looking back at the executives in their 'ivory tower' and saying to themselves, 'They have no idea!', and they try to influence the executive. And poor middle management is caught in the middle.

It's like what happens when two magnets are brought close to each other when the poles are reversed (figure 8.1). The flow of the magnetic field from north to south is interrupted. Getting risk appetite right is the beginning of alignment of the poles, where decisions are made within appetite, or are escalated if they are not, and information is fed back to decision makers to increase the knowledge and overall capability of staff throughout the organisation.

I believe risk appetite matters. BUT it is not as easy as saying, 'Let's have one.' I'll explain more about the challenge then provide you with some insight into how you can help your organisation develop or improve its risk appetite statement.

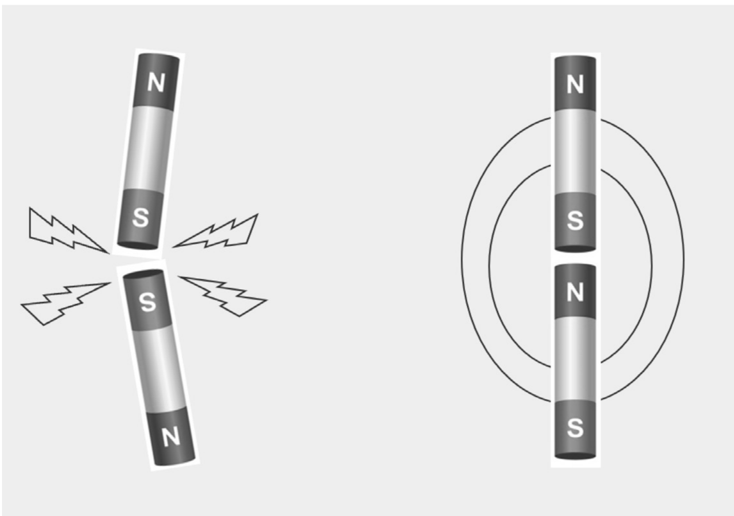


Figure 8.1: Risk appetite — aligning the poles

What makes it difficult?

Before I go into why it's difficult to document a risk appetite statement, let me say this: helping organisations with risk appetite is the single hardest thing I do. Full stop! It is hard to articulate, harder and often emotional to achieve agreement. Let me give you an example from when I assisted the board of a health district here in Australia.

Your typical health district runs hospitals as well as a range of community services to promote health and manage issues such as mental illness within the community. The boards are made up of clinicians, administrators and community representatives.

> I battled hard with this board to get a genuine risk appetite statement agreed. It took three sessions over a couple of months.

I battled hard with this board to get a genuine risk appetite statement agreed. It took three sessions over a couple of months. At the very end, as the ink was drying on the final agreed document, one board member said, 'I don't see why we can't just have one paragraph!'

Let me put this in perspective. First, the desire to go for one paragraph is admirable; indeed, I preach simplicity in risk. However, managing uncertainty requires a certain amount of rigour. Second, the board member probably felt comfortable having one paragraph because he had been in the room for all the discussions we had around risk-taking. A few small examples:

- The first position was that all of the strategic objectives, from acute care through mental health services through population health, were 'essential'. When I asked which ones would be discontinued if a pandemic hit the area and 30 per cent of staff were off sick while demand for services had gone off the charts, they soon realised their appetites for achieving certain goals were quite different.

- Patient safety with regard to the behaviours of some clinicians. Doctors work long hours. Some ignore guidelines on managing fatigue and press on regardless. Was this acceptable or not? Things to consider were whether the fatigue guidelines were appropriate and the potential backlash from doctors if they were held to account for breaching fatigue guidelines.
- Keeping the lights on. Recently there had been several power outages that disrupted one of the main hospitals. A report had been prepared that recommended a relatively large investment in backup power, money that could be spent on mental health or combating smoking and drug abuse. What was the board's appetite for risk of a disruption of several days to a hospital vs more funding for key services?

These issues need discussion and appetite for risk agreed. The hard part is then articulating it so decision makers can understand it well enough to apply it in similar and not so similar circumstances. That is why I always draw up the model for boards and executive teams shown in figure 8.2. The model helps discern the quality of a risk appetite statement. I ask the board and/or executive which type of statement they want. One that is fluffy and false and

The hard part is then articulating it so decision makers can understand it well enough to apply it in similar and not so similar circumstances.

damages the culture, or one that is convenient, uninspiring and will change nothing. *Or* one that is genuine, enduring and will help strengthen the culture of the organisation.

Of course the reply is always genuine and enduring. Then they fight tooth and nail to avoid words and statements that are anything more than uninspiring rhetoric, such as:

- We have a very low appetite for safety risk.
- We have a high appetite for innovation using technology but a low appetite for cyber risk and for disruptions to technology services.

> Yes, it is difficult to articulate risk appetite. I have seen 'more blood spilt on the boardroom floor' from discussions on risk appetite than on any other topic.

My question to them at this point is, who doesn't?

Yes, it is difficult to articulate risk appetite. I have seen 'more blood spilt on the boardroom floor' from discussions on risk appetite than on any other topic. So don't go into this thinking it will be easy or without collateral damage. I believe it is worth the risk, though.

The next sections will make your job a little easier, though it won't be risk-free either for you or for others involved.

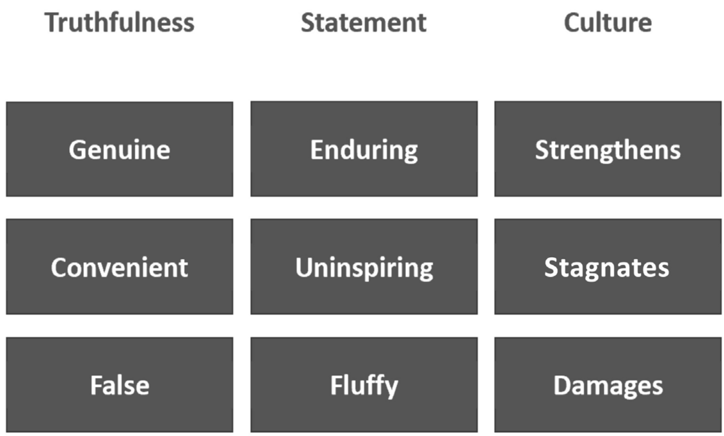


Figure 8.2: Quality of risk appetite statements

Risk appetite framework

I know, I know, another framework. Yes, I see risk appetite as needing its own framework so the main enterprise risk management framework is smaller and less daunting for staff. Yes, the risk appetite framework is positioned within the risk management framework so staff know it exists and where to find it, but it is not a focus for all staff. Just senior decision makers. The reason for this is that I believe risk appetite is set by the board, championed by senior management, operationalised by middle management and lived by staff (see figure 8.3). In practice, staff need to be guided to make decisions within risk appetite through policies, processes and systems. And middle management need enough understanding of appetite so that they can implement the needed policies, processes and systems to drive the organisation towards strategic goals. This is what I refer to as operationalising risk appetite.

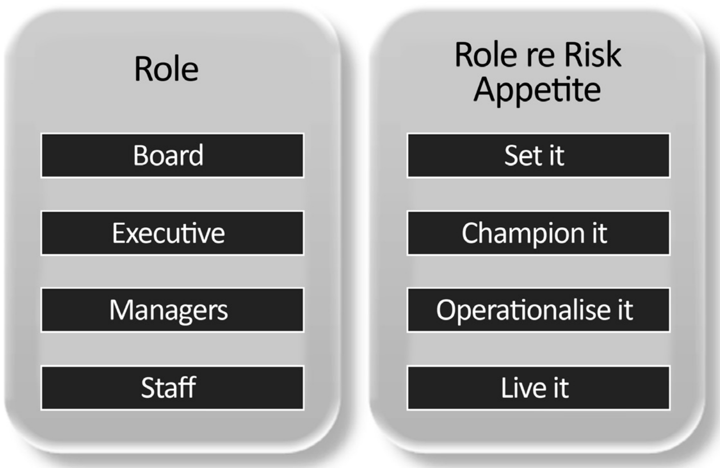


Figure 8.3: Risk appetite by role

Before I explain how to develop a risk appetite statement, let's examine the three components of a risk appetite framework: capacity, appetite and tolerance (see figure 8.4).

Capacity

This term relates to your organisation's ability to take on risk. With any risk decision you have to think about your ability to manage the business to achieve the core objective, to manage the uncertainty around it and to bear the consequences if the risk event does eventuate.

Appetite

A formal definition in the international standards is the 'amount and type of risk that an organisation is willing to pursue or retain' — in other words, what we are willing to risk to achieve the goals we have set. For example, are you willing to partake of a local custom of 'facilitation payments' to government officials to win government contracts? This might give rise to a moral or values-based type of appetite for risk. Or, are you willing to lose $7 billion in pursuit of a new treatment for breast cancer? You may choose to take such a financial risk because of the potential upside and your confidence in the research team developing the treatment.

A formal definition in the international standards is the 'amount and type of risk that an organisation is willing to pursue or retain' — in other words, what we are willing to risk to achieve the goals we have set.

The challenge with appetite is always expressing what is an intricate subject comprehensively but succinctly when developing a risk appetite statement that is genuine and enduring, and that strengthens your organisation's culture.

Tolerance

This is about the setting of boundaries. The process of establishing the minimum and the maximum risk to be taken in pursuit of your objectives. The line in the sand you must cross and the line in the sand you will not cross. For example, 'We must invest $3 billion over the next three years to find a new treatment for breast cancer. However, we will not exceed a total commitment of $5 billion over the same period.'

Tolerances are relatively easy to determine when it comes to financial risk. It gets harder when talking about people's lives or customer service.

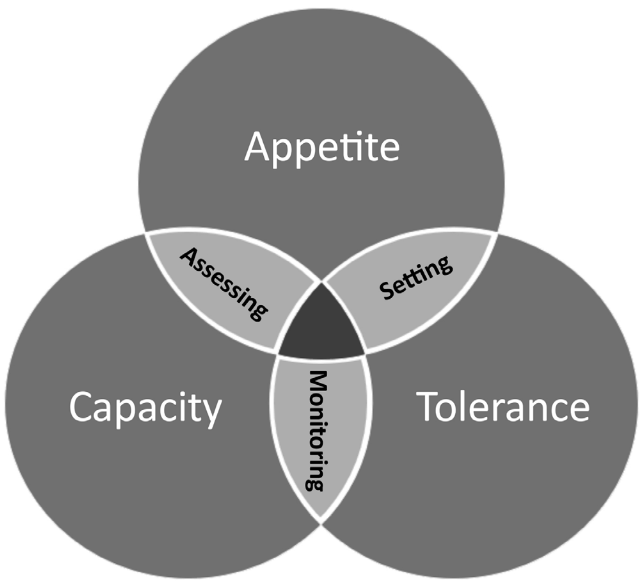


Figure 8.4: Risk appetite framework

Developing risk appetite statements

Refer again to figure 8.4, which shows the relationship between each of the three key components of the risk appetite framework: assessing, setting and monitoring. The organisation's appetite for risk taking can only be set based on an assessment of the organisation's ability to take on risk. Once you have set your appetite, you need to monitor the organisation to confirm whether you are operating within the agreed appetite for risk taking.

When I help leaders of an organisation assess organisational capacity to manage risk, I conduct a risk maturity healthcheck.

Assessing capacity

To assess your organisation's capacity to take risks, you need to consider the ability to manage risk and the ability to withstand the impact of events should they arise. Being good at managing risk does not mean bad things will never happen.

When I help leaders of an organisation assess organisational capacity to manage risk, I conduct a risk maturity healthcheck. The assessment looks at five key building blocks that make up an organisation:

1. Strategy & Performance
2. People & Knowledge
3. Processes & Systems
4. Assets & Liabilities
5. Capability & Culture

> This risk management maturity model is different from most as it is not an assessment of your progress in implementing technically correct risk management guidelines, using language like *basic* or *repeatable* or *optimised*.

This risk management maturity model is different from most as it is not an assessment of your progress in implementing technically correct risk management guidelines, using language like *basic* or *repeatable* or *optimised*. It is an assessment of how agile your organisation is in making risk-based decisions. The five maturity levels I use come from the S-curve I introduced in chapter 5 (figure 5.2), where Agile is the most mature level. I have found this methodology to be very helpful for senior leaders as they will much more readily assimilate words like *vulnerable*, *adaptive* and *agile* than basic, repeatable or optimised.

The rating system takes each element and breaks it down into the five sub-elements shown in figure 8.5 As you can see, these are standard elements of an organisation. The maturity assessment is not an assessment of whether an organisation has a risk process that has resulted in the development of risk registers or other typical artefacts of risk management frameworks. It is an assessment of whether the organisation has put in place suitable processes for managing uncertainty in pursuit of organisational objectives. This might sound complicated but it's important. Let me explain.

Remember my discussion with the Company Secretary of a large corporate about how they managed projects successfully, recounted in chapter 5? The answer given was Red Teaming, bringing in a review team on a major project to see how well the project was planned or was progressing. When assessing an organisation's project risk management, I would rate them favourably if they were doing Red Teaming very well, particularly if they were rating risks identified in the process using the organisation's approved risk criteria. Risk management can be achieved in many different ways, but fundamentally it is about quality over 'correct' application of guidance documents like ISO 31000.

Another piece of the risk appetite puzzle that deserves to be highlighted is the ability to bear the consequences of risk. In my risk maturity healthcheck I address this through the sub-elements of asset and liabilities. These sub-elements highlight for senior leaders how vulnerable or resilient their organisation is to the impact of risks occurring. A strong balance sheet is obviously key, but so are the other sub-elements that protect the balance sheet. That might be anything from insurance and management of potential legal liabilities, through strong contract negotiation and documentation and

> The ability to manage uncertainty should be a key consideration when determining strategy and setting targets.

ensuring key assets (tangible or intangible) are managed effectively over the long term, to allowing for timely renewal of fixed assets and financial planning as intangible assets lose their legal protection or competitors catch up.

A solid assessment, such as my risk maturity healthcheck, drives the critical conversations you need to have with your board and executive team *before* risk appetite is set, and, in an ideal world, *before* the organisation's strategy is set. After all, the ability to manage uncertainty should be a key consideration when determining strategy and setting targets.

<table>
<tr><th colspan="2">Element</th><th colspan="2">Sub-element</th></tr>
<tr><td rowspan="5">Strategy & Performance</td><td>Governance Framework</td><td rowspan="5">Process & Systems</td><td>Operational Risk Assessments</td></tr>
<tr><td>Strategic Analysis</td><td>Resource Planning</td></tr>
<tr><td>Strategic Risks</td><td>Project Management</td></tr>
<tr><td>Risk Appetite</td><td>Change Management</td></tr>
<tr><td>Reporting Regime</td><td>Compliance Process</td></tr>
<tr><td rowspan="5">People & Knowledge</td><td>Resource Planning</td><td rowspan="5">Assets & Liabilities</td><td>Physical Asset Risk Management</td></tr>
<tr><td>Induction</td><td>Intangible Asset Risk Management</td></tr>
<tr><td>Capability Development</td><td>Balance Sheet Risk Management</td></tr>
<tr><td>Performance Management</td><td>Insurable Risk Management</td></tr>
<tr><td>Knowledge Management</td><td>Legal Liability Management</td></tr>
<tr><td colspan="2" rowspan="5">Capability & Culture</td><td colspan="2">Accountability</td></tr>
<tr><td colspan="2">Decision Making</td></tr>
<tr><td colspan="2">Resourcing</td></tr>
<tr><td colspan="2">Communication</td></tr>
<tr><td colspan="2">Metrics</td></tr>
</table>

Figure 8.5: Risk maturity healthcheck rating elements

Setting appetite

There is no right or wrong answer to how you set appetite. I will say, however, that I think documenting risk appetite by risk category only is incomplete. Every risk appetite statement should be linked to strategy. I have developed and trialled several methods over the years. They boil down to three key types of statements:

1. **A general statement.** A statement reinforcing the values of the organisation and highlighting the risks that need to be taken and those the organisation tries to minimise. The statement typically is about one page in length and covers the key areas of safety, finance and regulatory compliance. It also highlights the types of activities, such as in research and development, that must be undertaken if the organisation's purpose is to be fulfilled.

   I usually recommend this approach if the organisation's risk maturity is low. Recognising that they are all difficult to reach agreement on, this is the least difficult and so produces less friction between board and executive, within the board and among the executive.

2. **An objectives-based statement.** One written statement for each strategic objective describing the minimum and maximum amount of risk to be pursued in working towards achieving the objective. Often this approach will include examples of the types of activities there is a strong appetite to

pursue and others that are to be avoided if possible. This approach is also often accompanied by visual indicators of risk appetite, such as traffic lights.

I recommend this approach for mature organisations that want a robust discussion and deeper clarification of the risks to be taken and those to be avoided. It requires strong facilitation skills to minimise friction and to ensure all involved buy into the end product. A strong advantage of this approach is that it provides greater guidance to management, which makes it easier to discover what can be measured and to identify if the organisation is operating within the defined appetite.

3. **A swim lanes approach.** In this approach, four levels of risk appetite are described, such as *controlled*, *cautious*, *accepting* and *open*. These become swim lanes. Appetite for risk-taking is set by placing each strategic initiative, along with key programs and frameworks, into one of the swim lanes. For example, a strategic initiative to open an operation in a new country might sit in any of the lanes depending on the size of the investment and the view on how capable the organisation is to deliver. For

> Appetite for risk-taking is set by placing each strategic initiative, along with key programs and frameworks, into one of the swim lanes

something like regulatory compliance in a heavily regulated industry, the compliance program may sit in the most risk-averse lane, *controlled*. Similarly, for a government entity the procurement framework might sit in the *cautious* lane while for an innovative private-sector company it might sit in the *accepting* or *open* lane.

Once appetite is set using descriptors, it is common practice to establish a set of risk tolerances that are often called key risk indicators (KRIs).

The advantage of this approach is that it is highly visual and requires much less careful use of appetite descriptors. It works best for organisations that have well-defined strategic initiatives, programs, projects and frameworks. It also promotes an understanding that some new initiatives may naturally have to have an open or accepting risk appetite. As the maturity of the initiative increases, its upside and downside will become clearer and may become more controlled.

You can find examples of each of these types of statements in the learning resources section of my website bryanwhitefield.com.au/learningresources.

Monitoring performance

Once appetite is set using descriptors, it is common practice to establish a set of risk tolerances that are often called key risk indicators (KRIs). As with every aspect of risk, it seems to be easier to focus on the downside; however, understanding risk appetite is as important for ensuring your organisation seizes the right opportunities — that is, takes sufficient risk to be successful in the long run. The late 'systems thinker' Dr Russell Ackoff once wrote, 'The deterioration and failure of organizations are almost always due to something they did not do.' KRIs should be set with lower and upper limits.

For example, an organisation may decide that there should be a healthy level of ongoing innovation. In this case, you could set a lower and upper financial limit of investment in innovation projects. If the level of investment is tracking below the lower threshold, questions might be asked. It may be that there is too much red tape for new projects or that funding has been pulled for one reason or another. Either way, management can investigate and decide if action is required or if it is acceptable to operate outside appetite for a while.

If the organisation consistently operates outside of the agreed tolerances, then the capacity they thought they had must not be there.

This leads to a point I like to make to boards and executive teams. Tolerances are there to measure whether or not they were right when they assessed the organisation's capacity to manage and bear risk. If the organisation consistently operates outside of the agreed tolerances, then the capacity they thought they had must not be there.

They will either have to shift appetite or do something to build capacity.

Being an engineer, I am a measurement kind-a guy. I'm not afraid of numbers and I love the challenge of quantifying difficult things. If you do too, I highly recommend *How to Measure Anything* by Douglas Hubbard. In his words, if you can observe it you can measure it. Whether you pursue measurement comes down to the cost of acquisition of the ability to measure vs the value it will deliver.

Whether you pursue measurement comes down to the cost of acquisition of the ability to measure vs the value it will deliver.

Herein lies the trap when it comes to KRIs. Sometimes there is a tendency to overcomplicate things by measuring too many indicators, because there are so many indicators you can measure. Take financial indicators, for example. There are sales stats, cost of goods sold stats, liquidity ratios . . . and on it goes. Most may already be measured, and for good reason. They may be used to fine-tune performance of the sales team or the supply chain, or to demonstrate financial stability to creditors. When it comes to developing KRIs, I suggest measuring the bare minimum. Let the business fine-tune and only worry about the big-ticket items.

When it comes to sales, for example, can you do some modelling to find out the biggest indicator of future sales? Is it the unemployment rate, the weather or the number of hits on your e-commerce website? If it is a good enough indicator, just monitor that. Sometimes it won't be just one thing. For example, cost of goods sold might vary based on oil price, weather and lead time for order fulfilment. In such a case, measure all three but report it as one KRI. That is, the COGS (cost of goods sold) KRI.

Help them see the benefit of data and indicators to fine-tune their business. You are a risk partner, not a surrogate manager of their business.

There is no need to get bogged down in the detail. Leave that to the fine-tuning of performance in the business. The role of risk tolerances is to let the business run its game and only raise a warning if necessary. By the way, if the business does not do fine-tuning using metrics well, don't try to fix it using risk appetite. Help them see the benefit of data and indicators to fine-tune their business. You are a risk partner, not a surrogate manager of their business.

And don't fall into this trap. One client I worked with followed the objectives-based statement method. For each statement we were able to identify one or two KRIs, for which we set lower and upper boundaries. The problem was that some of the KRIs were measured only annually or bi-annually. So when it came to reporting time, either there was nothing relevant to report, because the data was out of date, or a whole heap of work went into trying to measure it.

One last item on the topic of tolerances. Can you measure culture? The answer is yes. Culture is observable. Therefore, as per Hubbard, it is measurable. The question for you is, is it worth measuring any more carefully than how overall culture is traditionally measured — via a culture survey? In some organisations, such as those regulated by APRA and those who experienced a Royal Commission into misconduct, it is. Misreading your culture and having major issues that draw the attention of the regulator or, worse, the media, could be career limiting for many involved.

> The question for you is, is it worth measuring any more carefully than how overall culture is traditionally measured — via a culture survey?

Operationalising risk appetite

I mentioned earlier that risk appetite is set by the board, championed by senior management, operationalised by middle management and lived by staff. In practice, this means staff need to be guided to make decisions within risk appetite through policies, processes and systems. And middle management need enough understanding of appetite so they can implement the needed policies, processes and systems to drive the organisation towards its strategic

> The method I use for operationalising risk appetite, in order to use it to influence decision making, I call decision mapping.

Once a decision map is prepared, policies, processes or systems can be prioritised for development or improvement as required.

goals, which is what I refer to as operationalising risk appetite.

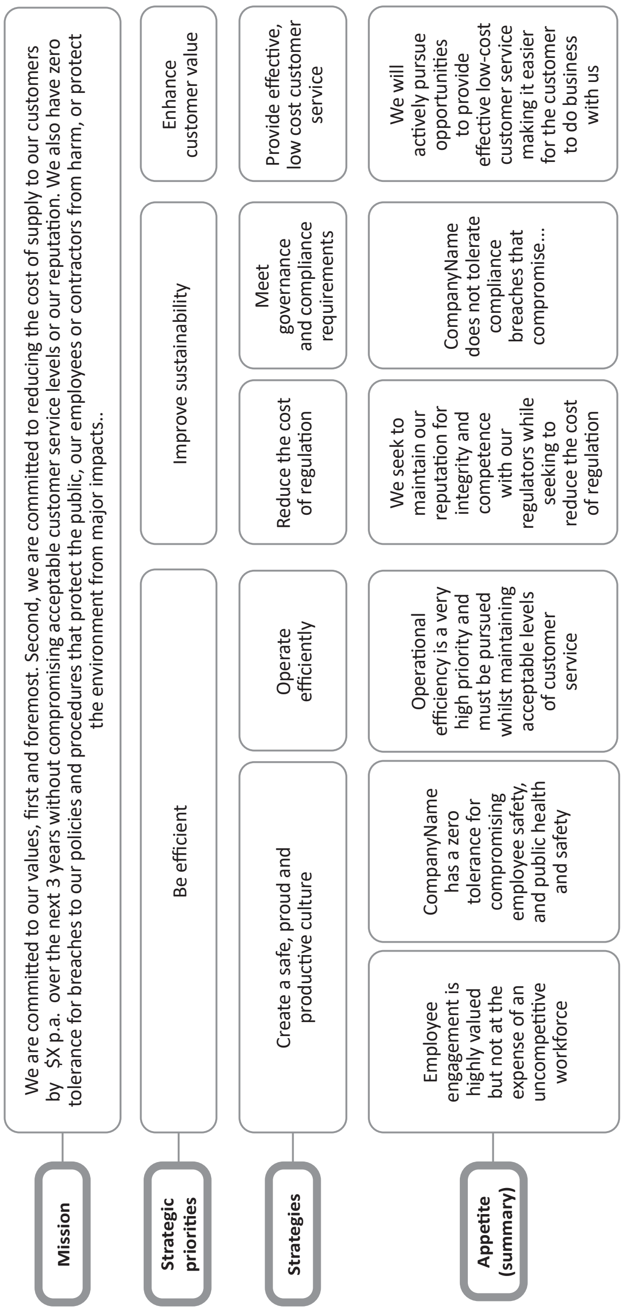
The method I use for operationalising risk appetite, in order to use it to influence decision making, I call decision mapping. It means the development of a decision map that documents the policies, processes and systems in place and their ability to guide decision making within appetite for risk. Once a decision map is prepared, policies, processes or systems can be prioritised for development or improvement as required. An example of a decision map is shown below in figure 8.6. The map starts at the highest level, the organisation's strategic goal or mission statement, and works down to strategic priorities and the appetite statement for each priority. From there the *translation points* for the appetite statement are the key organisational policies and frameworks, such as the performance framework, procurement, finance and HR. Each one is then assessed as to whether or not it clearly guides staff to operate within appetite for risk. The classic examples are financial delegations and procurement frameworks — who is able to sign off on what and within what limits.

Once you have identified policies, processes and systems that need improvement, the rest comes down to how urgently you need these improvements and the resources available.

If your organisation is performing reasonably well, I would urge you not to rush it. It will be better in the long run if you design changes that are as simple but effective as possible.

In the next chapter I discuss the challenges of monitoring your organisation to see that it is within risk appetite and some practical tools for further linking risk appetite to strategy.

> Once you have identified policies, processes and systems that need improvement, the rest comes down to how urgently you need these improvements and the resources available.


Mission
We are committed to our values, first and foremost. Second, we are committed to reducing the cost of supply to our customers by $X p.a. over the next 3 years without compromising acceptable customer service levels or our reputation. We also have zero tolerance for breaches to our policies and procedures that protect the public, our employees or contractors from harm, or protect the environment from major impacts..
Strategic priorities
Be efficient
Improve sustainability
Enhance customer value
Strategies
Create a safe, proud and productive culture
Operate efficiently
Reduce the cost of regulation
Meet governance and compliance requirements
Provide effective, low cost customer service
Appetite (summary)
Employee engagement is highly valued but not at the expense of an uncompetitive workforce
CompanyName has a zero tolerance for compromising employee safety, and public health and safety
Operational efficiency is a very high priority and must be pursued whilst maintaining acceptable levels of customer service
We seek to maintain our reputation for integrity and competence with our regulators while seeking to reduce the cost of regulation
CompanyName does not tolerate compliance breaches that compromise...
We will actively pursue opportunities to provide effective low-cost customer service making it easier for the customer to do business with us

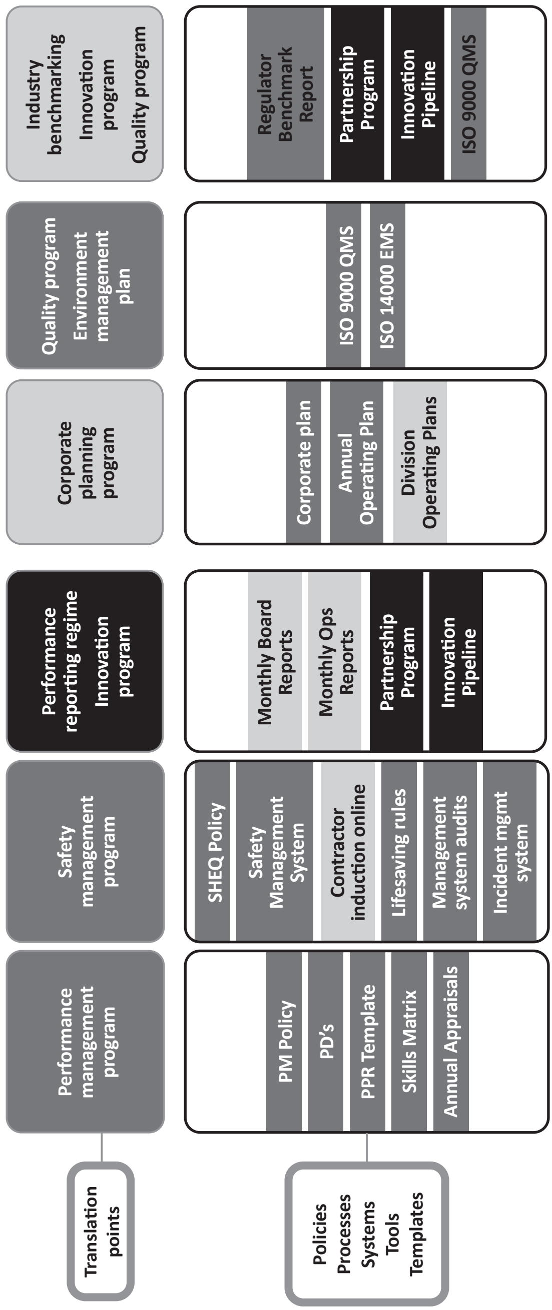


Figure 8.6: Sample decision map