You've got a risk register? Mind if I have a look?

Collectively, we invest a lot of time and effort doing risk assessments. They're done for different purposes, using different frameworks, and with varying degrees of competence and enthusiasm. Some are simple, some complex. Some are captured in dedicated risk management information systems, some in Microsoft Excel, some in a funky SharePoint database developed by a long-departed intern/graduate/vacationer who needed a project. These risk assessments, risk registers or risk profiles (I will use these terms interchangeably through this article), are the analysis and recording of a set of uncertainties – things we need to manage to be successful.

I get asked to review a lot of them and there's a question I have to ask - why do they rarely support decision making and action in practice? Why are they so often viewed as compliance and reporting activities? 'Spreadsheets of death' - places where risks go to die.

Regardless of the framework or system it's developed within, I believe there are enduring qualities that suggest whether a risk assessment is likely to be useful in practice or a comforting placebo. In this brief article I offer 12 tests you can apply to any risk assessment you encounter.

Is the assessment linked to what must go right, or is it just a list of things that can go wrong?

Risk is the effect of uncertainty on objectives. Accordingly, you should never disconnect what could go wrong from what must go right.

A list of perils without a balancing link to objectives becomes an exercise in paranoia and risk aversion. Risks can become a paralysing list of the anxieties of the day.

No risk should be accepted or declined without a clear understanding of the size of the prize potentially gained or lost (including by choosing not to engage with the risk). In practice this can be achieved by ensuring every risk is linked to a measure of success. This can be done by attaching objectives to your each of your risks or attaching risks to your objectives.

Is it prioritised, are the important things first?

I had a group of managers who had worked hard to develop their risk profile. I put the risks up on a projection screen and asked them "if you were in the elevator with the Big Boss, and he/she asked what risk was like in your division, and you had 30 seconds to answer, which of these risks would you talk about?" Their answer was immediate – "we'd talk about risk #8, that's the big one!". Why is it risk #8 then?

You can't keep reordering your risks constantly, but the profile should start with the biggest or most urgent concerns and work its way down to the important, but otherwise unremarkable, risks last.

Similarly, other information attached to the risks should be prioritised. For example, critical controls described first followed by lesser important ones. Often these lists become overly long as people dump everything into them. Ordering them helps cull trivial entries and give a sense of relative importance.

Prioritisation is particularly important when reporting risk to Boards or senior committees. Never give a senior audience the 'big spreadsheet'. They won't have time to read it, probably won't understand it, and will skim until they find a spelling mistake on page 4 and this is what they will want to talk about. These reports should be tiered. They should have a brief executive summary that documents the top two to four key concerns and major changes. This sits over a dashboard that describes the most critical information, and after this, only then, is the detailed information made available.

Have the right people had input to it?

Regardless of how nice the risk profile looks, have the right people or organisations contributed to it? The "the boss asked me to do a risk assessment, so I shut the door for four hours and here's what I produced" risk assessment is unlikely to be worth the paper it's printed on. It will be completely corrupted by the human biases, expertise and ignorance of that one author.

Remember that the conversations had during a risk assessment can be more useful than the risk profile produced. Similarly, even if a particular stakeholder "wouldn't have added anything new", their involvement in the process can make the final product much more acceptable and authoritative.

Are there the right number of risks?

There is never a single 'right number of risks'.

But it is 10.

Ok, not exactly 10, but my experience is that any set of risks numbering much beyond this is not being actioned by anyone other than a dedicated "risk manager" who has nothing else to do (not that this is how you want risks controlled anyway). It is better to manage 10 risks well than 50 risks badly.

If you have many more risks than this, you may be breaking each one into too much individual detail and not looking for common themes.

In complex organisations or programs where there are clearly more than 10 risks that need managing in a structured way, the risk profiles should be tiered. 10 (ish) at the top level, then sets of 10 delegated into the business or across projects. Business rules and constant communication ensure strong linkages between the risk profiles across the organisation and at different levels and allow for escalation and delegation of risk.

Does the profile highlight change or trends?

Risks are never static and understanding change is as important as understanding the current state. A risk assessment that is purely a snapshot in time gives no sense that the situation is improving or getting worse. If I am to accept or reject a risk, I want to understand how it is changing. It's a bit like if I am planning an outdoor party this weekend, a weather report that solely says "it's not raining at your house now" is largely unhelpful.

Consider including a data element for each risk that shows how that risk is moving. Is it getting more or less severe? Have there been significant changes to its sources or the control environment? Are any forecast?

Does it contain the right level of detail?

We manage risk on a spectrum of rigour - sometimes we need thorough and detailed analysis, other times we need to equip time-poor decision makers as simply as we can. There is no ideal risk information set, nor is there a single set that will suit your organisation at all times and at all levels. My article "*Is the devil in the detail, or is the detail the devil?"* discusses some risk information that can be included in a risk assessment (where they add value). A fitness for purpose test needs to be applied.

Some risk registers look like they've been populated by a 'drop-down box' selector trying to set a speed record. Indeed, some dedicated risk information management systems can enable 'click-and-forget' selection of risk information. Controls (for example) described as "good communication", "staff training" or "document filing" by themselves are not controls, they are generalities that are not specific, measurable or able to be assured.

There is a balance here between specificity and clear language. The complexity of any risk assessment should be commensurate with the complexity of the risk environment.

How does the profile capture control-critical risks?

Severe risk is not bad risk and low risk is not good risk. I write this in almost every article I publish.

Yet, I've seen risk registers and risk reports that excluded risks with lower current severity by rule. This removes control-critical risks from the formal risk management and assurance process. Control-critical risks are those which may be currently low or medium severity today but are critically dependent upon the continued effectiveness of the controls in

place. If these risks are removed from the risk framework, what management process will ensure this continues?

Any risk assessment should capture risks which are both high today, and risks which have been assessed as inherently severe and control-critical, so may be low today.

How does it allow for outliers?

Any system of analysis needs to cater economically for the majority of cases, but not neglect the minority. A process that works for 100% of situations will be incredibly inefficient at dealing with the 80% of cases that dominate. The same is true of risk. A process that efficiently helps a project manager think about the various things they need to manage for their project to be successful isn't likely to be useful for analysing outliers such as critical incidents.

There will be risks for which the mainstream process doesn't provide good analysis. High consequence, but very low likelihood risks are a good example. How does the risk assessment process deal with unusual risks such as internationally disruptive events, natural disasters or wholesale change in the operating environment?

Do the people using it actually understand it?

I reviewed a very impressive looking risk register once. Its design was full of subtle detail and interesting data elements. Clearly, it had been originally designed by someone with a deep understanding of risk mechanics. However, speaking to the people who actually populated, managed and implemented it, it became apparent that no one understood what much of it meant! They were filling in information based on the rows above and guesses as to what each individual thought the element meant. Their risk framework was also silent in defining many of the concepts.

Any risk framework or process needs to be understood by the people who own it. These people will come and go and may have no background in the science and art of risk management. Ask if the terms and concepts in the risk assessment are defined and consistently understood. Is ongoing training or support being provided to ensure the maintenance of the risk profile doesn't degenerate into guesswork?

Does it consider the risks as a profile or just a set of individual risks?

Any risk register is more than a set of individual risks. They form a risk profile that is more than just the sum of its parts. Inter-dependencies and linkages between risks can lead to many being realised at once from a single trigger or for cascading effects. 10 medium level risks can be as bad as nine low risks and one extreme one.

Connections and relationships between risks should be called out. Similarly, common or pervasive sources and controls (those that influence several risks) should be identified. If a single risk source could trigger multiple risks, it needs careful management and proactive monitoring. If a single control helps manage a number of risks, it needs protection and resourcing. In aggregate, the risk profile should tell a story of the health of a subject and not just be 10 individual unlinked diagnoses.

To achieve this, someone needs visibility and authority across the whole risk profile, not just each individual risk.

Does it drive action and accountability?

I love a risk assessment that describes dozens or hundreds of actions (controls and treatments in risk language), none of which are assigned an owner/implementer.

First-aiders are taught to never yell "someone call an ambulance!", because no one will. They are instructed to point and yell "you, the guy in the red shirt, you call an ambulance!" and get an acknowledgement that red shirt guy can and will. Just like this, accountability is everything in risk management. If no one is assigned accountability for an action (or worse, a loose group of people are assigned), nothing will be done and there will be no accounting for it when the risk is inevitably realised.

Importantly, many risks controls and treatments are implemented by others on your behalf. Do they know and accept they have this responsibility and the potential effect on the risk should they stop doing it? What ensures this doesn't happen next time the control implementer has a big restructure, cost-reduction or crisis of their own?

Is it living and used in practice?

There is a joke that "the Queen must think the whole world smells of fresh paint". The rationale being that everywhere she visits is freshly repainted before she arrives. I often think the same of risk assessments – freshly updated before the reviewing consultant arrives, but ignored in the months before.

Ask how is the risk assessment discussed, debated and challenged? How is its actual implementation in practice assured? And, not just by some "risk manager", but by the management team accountable for the objectives the risks make uncertain? Managers make risk decisions every day, but too often these are divorced from the risks captured in the structured system. If this is the case, why maintain structured risk management arrangements at all?

In reviewing a risk assessment, ask how it is converted into tangible actions and outcomes - "what have you done differently this month because of this risk profile?" Or, is it just an exercise in documentation?

Summary

In closing, there is no single way to undertake a risk assessment, build a risk profile or document a risk register. There are though a number of common attributes that any set of risks should have. Apply these tests next time you look at one.

First published 14 July 2020, v1.0

Sal Sidoti has over 30 years' experience working with public and private sector organisations across Australia and further afield. He works with his clients providing tailored risk management advisory services that support decision making in practice. Approaches that go beyond cut-and-paste compliance and death by spreadsheet. Sal is the Director and Principal Consultant of Crafted Solutions Pty Ltd. He is home based near Canberra, Australia.

https://au.linkedin.com/in/sjsidoti
enquiries@craftedsolutions.com.au

Title illustration courtesy of the National Cancer Institute via Unsplash