Is the devil in the detail, or is the detail the devil?

How much risk information balances benefit and burden?

More information provides greater detail and allows more analysis which leads to better insight. More insight means a decision advantage, and who wouldn't want that? Richer and more diverse risk information sources provide quality and enable trust. Having more information can be a real winner. Right?

But, some information can be expensive and difficult to collect, and time consuming and confounding to analyse. It can perish before we use it and be manipulated to mislead. It can cloud gems of insight with layers of 'noise'. It can overwhelm our ability to process, communicate or digest and lead to risk reports too dense to read. More information can be a real pain. Right?

In theory, considering a fuller range of risk attributes should allow you to manage it better. I sometimes pose the following scenario in my workshops and training programs - a friend rings you out of the blue and asks a simple question "Hey buddy, I'm in a car and I'm doing between 50 and 80 km/h, what should I do?" The response from the group is always that it is not possible to provide any meaningful advice other than to respond with a series of questions - where are you, where are you going, what sort of car are you in, what is around you, etc, etc, etc. Making a good or valid decision based on a single narrow data point is hard. Yet, often, we use the single data point of current or residual (today's) risk to do just that, "Hey buddy, I've got this HIGH risk, what should I do?"

So, it isn't difficult to agree that in theory, more risk information is "other-things-being-equal" better. However, sometimes we need to act quickly and make risk decisions intuitively. We rarely have the luxury of considering a single risk in splendid isolation. Even if we are disciplined in focusing on our 'top 10', there remains a need to be as streamlined as possible to avoid the perception of being a burden.

However, as Daniel Kahneman says in his book *Thinking Fast and Slow* "The spontaneous search for an intuitive solution sometimes fails – neither an expert solution nor a heuristic answer comes to mind. In such cases we often find ourselves switching to a slower, more

deliberate and effortful form of thinking." We manage risk on this spectrum, sometimes we need rigorous and detailed analysis, other times we need to equip time-poor decision makers as concisely as we can.

So, 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. I've seen organisations ground to risk management paralysis by trying to include too many data points in their risk registers. The whole thing became a cumbersome overly complicated burden. What we need is to be able to pick and mix to suit our needs. What are some risk information elements that you can consider for inclusion (or exclusion) in your approach? Here are some examples:

Inherent risk. Few things divide the risk community more than the concept of inherent or pre-control risk. Inherent risk is how big and scary the risk is assuming we are doing nothing deliberate to manage it. Yes, it is a hypothetical level of risk because it assumes we strip away the things we (and others on our behalf) are doing to manage the risk right now. Inherent risk though is an incredibly useful indicator of how much we should care about a risk regardless of how well we think it is currently being managed. High inherent risks that are considered well controlled are the most dangerous risks we face, as overconfidence in ineffective controls is the single biggest cause of risk realisations. Starting with the position of inherent risk helps us identify these risks when they may be otherwise overlooked as under control and off the radar. As useful a tool as inherent risk is in supporting risk assessment, it is more a means than an end. Be careful including inherent risk in reports if your audience doesn't understand the concept – it can create significant confusion.

Links to objectives. Every risk conversation should start with the question "what does success look like to the people who matter?". Failing to identify what must go right first will compromise the risks you identify. Hence, there can be value in explicitly noting which objectives are potentially affected by each risk. Objectives can be drawn from your strategic priorities, agreed outcomes or business planning. Once the linkages are in place, flipping the analysis to list risks against objectives can be useful. Objectives with too many risks may be at jeopardy from their aggregate influence, and objectives with no risks suggest that the risk assessment may have gaps.

Sources and Causal factors. Risk parsing is the act of describing a risk in terms of cause, event and consequence. Often though, our risks have many potential causes and many potential consequences. The higher in an organisation the risk, the more likely this is and diligently parsing your risks leads them to multiply. One method of managing this is to separately list sources or causal factors for each risk. Understanding why a risk exists, or what influences its severity is one pointer to how we can control it. Compare the preventative controls you have in place to the causal factors and the vulnerability any mismatch might leave.

Risk velocity and proximity. If you are made aware that you are exposed to a severe risk, you will immediately want to know how quickly that risk could be realised. The pace of change of the risk, or how quickly it could eventuate, are important measures of how much

you should care about a risk today. Again, the concept can be blurred with various interpretations of the terms. Other things being equal, the nearer the risk or the more rapidly it could change the more you should be interested in it.

Target risk. The term 'target risk' is used variously to refer to either where you want the risk to be or where you assess it to be once the described treatments are implemented. I prefer the former definition as I think it adds the most value by communicating our appetite for this particular risk. Not all risks can or should be driven to low, and some may be desirable to hold at higher levels. Comparing residual and target risk shows us how much more work we have to do and how tolerable the risk is.

Tolerability. In my article *Dr. Strangelove or: How I Learned to Stop Worrying and Love that Severe Risk* I talk about the value of separating risk severity from risk tolerability. Severity and tolerability are different things, and although in a well architected risk system they are tightly coupled, too many risk systems are not so well designed. High risk is not necessarily bad risk, and low risk is not necessarily good risk. A tolerability flag helps decision makers record their level of comfort with a risk, both now and in anticipation of the agreed treatment plan. And, if your risk framework only has four levels of risk severity (low, medium, high and very high, for example), a tolerability traffic light can help draw attention to risks of concern, noting that 80+% of your risks are likely to be crowded into the two middle severity ratings.

Current controls and proposed treatments. As I suggested earlier, I believe the vast majority of risk realisations in practice are caused by overconfidence in ineffective controls. The controls we (or others) are currently implementing and the treatments (proposed controls) we intend to implement are the one thing we can actually do to manage risk. Critically, these must be well described - "staff training" or "good communication" are good intentions not controls. They are imprecise, lack ownership and cannot be measured or assured. The more precisely you can describe a control and assign responsibility for its implementation the more likely it is to be effective in practice.

Change or trend. Risks are never static. Consider a data element for each risk that shows how that risk is moving. Is it getting more severe? Have there been significant changes to its sources or the control environment?

In summary, there is a tension between brevity and comprehensiveness when describing risk. If you are operating in an environment where people are able to intuitively make mature and nuanced risk judgements you can streamline your assessments and reporting. But sometimes you need the detail to manage complex risk. To test whether you are at the right point on the spectrum, ask the following questions:

- Is the rigour of our risk assessment process commensurate with the scale and complexity of our risks?
- How many data elements are rarely populated? Do we understand and utilise all the risk information we collect?

- How much do we want to, and are able to, conduct analysis across our risks to identify systemic issues and opportunities?
- Do we have different tailored risk reports for different purposes and audiences?
- How often are we actually doing things differently having reviewed the risk information we have? Is the risk information we collect, analyse, record and report generating the insight that helps us manage risk better?

Its about balancing burden with benefit, and each organisation and situation will have its own right answer. Like everything in risk management, it's about fitness for purpose and generating outcomes, rather than following rote process or copying the person next door.

First published 11 June 2018, 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 to design and implement tailored risk frameworks that support decision making in practice. Approaches that go beyond cut-and-paste ISO 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 images courtesy of Aaron Burden and Nicolas Cool via Unsplash.

