The Risk Management Drinking Game

I remember gathering in front of the Eurovision song contest on SBS and playing the Eurovision drinking game. There were many versions of the rules, but they followed a theme - every time you saw or heard something on a list of predictable Eurovision staples, you sip or scull your drink. An example was "a Velcro tear-off costume change half-way through a performance" - scull!

Inspired by this, I joke of the "risk management drinking game". That urge to chug a drink every time I hear someone earnestly roll off a dodgy risk management statement, "factoid" or myth.

This article makes light of a serious problem. People become captured by risk management beliefs that are either false or at the very least unhelpful in the circumstances. In this brief article I discuss ten questionable statements I often hear and some questions to reply with.

Risk Management Factoid #1 "That's not a risk, it's an issue"

A risk is an uncertain future event that may have an effect on an objective. An issue is something that has occurred with which we are dealing with the consequences. Sounds straight-forward, but real risks and issues are rarely that black and white.

Let's use the simple example of my personal risk of having a car accident. If I had a car accident this morning, does it cease to become a risk for me in the future? Unless the accident kills me, the answer is likely no. I need to manage this morning's crash as an issue but continue to manage the potential for another crash as a risk.

It is actually uncommon for the realisation of a real-world risk to entirely stop it remaining a risk in some form. It more often becomes both a risk and an issue. Many risks have broad sets of consequences and are commonly only realised in part. So, a risk can be half-issue if parts of it have been realised, the rest remains a risk.

Questions to ask in response to this factoid include:

- Has all of this risk been realised, or does some of it remain uncertain?
- Do we need to deal with the current realisation as an issue but continue to manage this as a risk into the future?

Risk Management Factoid #2 "Green risk is good, red risk is bad"

If I had to explain the dominant risk culture in many organisations to a five-year-old in a single sentence I'd state this myth - green risk [low current severity] is good, and red risk [high current severity] is bad.

Neither of these assertions is true. Only some risks really need to be green, and nothing significant is ever achieved without carefully engaging with some higher risks. The desire to have registers full of green risks leads to endemic mis-assessment and misrepresentation of risk, and inevitable unnecessary realisations. It also encourages a view that the goal of risk management is solely to minimise risk and to stop organisations from doing great things.

I explore this phenomenon in more detail in my article "*Beware the devil in a deep green sea. When green risk is not good risk.*" and discuss what I call risk greenwashing - deliberately or inadvertently making risks appear "greener" than they are.

A 'watermelon' risk is a severe risk that has been greenwashed - green on the outside and red in the middle. Neglected because they appear 'safe' these are the risks that will burn you every time. Green risks can be some of the most dangerous risks you are managing. Conversely, an honestly reported and acted upon red risk can be the best news you've had all day. By acknowledging and then actively managing a red risk, you can ensure it is not realised.

Questions to ask in response to this myth include:

- What assurance do I have that the controls you've described for this green risk are (and will remain) as effective as you claim they are?
- Does this risk really need to be so low? What are the costs and consequences of making it so low?

Risk Management Factoid #3 "Risk is based solely on likelihood and consequence; the Standard says so"

If I said to you "you are exposed to a risk with a high consequence, and it is moderately likely to occur" would you be happy to change your life based on that sentence alone?

No, you wouldn't. You'd come straight back to me with a barrage of questions. What's causing the risk? How confident are you, what evidence do you have? How close is it, how quickly could it happen? Why then do we base so many of our risk management decisions on consequence and likelihood alone? Especially when likelihood is often unknown or even unknowable for many real-world risks.

My article "*Likelihood – Risk Management's Favourite get out of Jail free Card*" explores the likelihood dilemma in more detail. It notes that actually the Standard suggests likelihood and consequence are only two of the things to be considered when analysing a risk.

Real world risk management can be complex. Basing risk choices solely on a severity rating computed from likelihood and consequence alone is simplistic and often misleading. For example, it can lead to (amongst other things) the Sheer Size Fallacy – "Risk A was accepted, Risk B is a smaller risk than A, therefore Risk B should be accepted". At its extreme, we end up with statements such as "You will have to accept this unsafe work environment since the risk it presents is smaller than the risk of being injured in a car crash, which you accept every day."

Questions to ask in response to this factoid include:

- What basis have you used to estimate the likelihood of this risk?
- How near is this risk, how quickly could it change or be realised?

Risk Management Factoid #4 "That's not a risk, it's a cause (or a consequence)"

The real world operates as a series of inter-connected causal chains. An event or circumstance leads to another event which leads to another event and so on. As such, the same event could be a source of risk to you, it could be a risk to you, or it could be a consequence you are exposed to. It just depends on the lens you want to use.

An example might be the event "failure of a particular IT system". If you are the supplier who sold the system hardware to the organisation, this could be a consequence of your failure to manage a production quality risk. If you are the IT department, it is likely one of your risks. If you are a manager who relies on that system to do your work, it is a potential cause for some of your risks. So, although it is an event that no one wants to occur, each person could be including it in their risk management in a different way. A simple "bow-tie" risk analysis is really useful here. Few things are ever only causes, risks or consequences, you just manage them with the right label to get the maximum value in each circumstance.

Questions to ask in response to this factoid include:

- For whom is this a risk, for who it is a cause, and for who is it a potential consequence?
- Have we placed the risk event at the point in the causal chain at which we can exercise maximum control?
- We've agreed this is a "thing" that needs to be managed, how much extra value are getting endlessly moving up and down a causal chain?

Risk Management Factoid #5 "Reputation is our biggest risk"

The reputation of both public and private sector organisations can be severely damaged by the most trivial perceived failing. This is the result of a frenetic and click-bait driven media

cycle, anonymous social-media trolls, endless issue motivated groups desperately offended by almost anything, dash-for-cash litigation, and an often-uninformed Facebook dependent public. Reputation is important and it can be fragile.

I suggest damage to reputation is usually best managed as a consequence, not a risk event in its own right. To do so, we need to understand what parts of our reputation we want to protect most dearly – reputation isn't a homogenous blob. And then, what risks could affect our reputation most significantly?

Having adequate mitigative (recovery) controls in place for these risks could mean we are criticised for the risk event occurring but applauded for our response.

Questions to ask in response to this factoid include:

- What are the key risk events that could lead to damage to critical components of our reputation? How well are we managing them?
- Do all of our people understand our strategic risks and how they personally contribute to their prevention or causation?
- Do we have adequate detective (e.g. social media monitoring) and mitigative controls in place to quickly identify and influence reputation impacts should one of these risk events be realised?

Risk Management Factoid #6 "Let's start with "what's keeping you awake at night?""

How many risk workshops have you been to where this is the opening question?

I'd suggest that if something is keeping you awake at night, you don't run a risk management workshop, you hire experts in whatever is keeping you awake and tell them to fix it.

The aim of a risk assessment is to help you understand the things that should be keeping you awake, but maybe aren't. The starting point for this is ensuring we understand what is important to the people who matter. We can then explore where there is uncertainty in our ability to achieve that. Grounded in this context the risk assessment can identify true risk exposures and not just the known anxieties and fears of the day.

Questions to ask in response to this factoid:

- Who are the people who matter to us, and what does success look like to them?
- Where is there uncertainty in our ability to achieve that success?
- What are we doing to manage that now, and what do we need to do differently to make it acceptable?

Risk Management Factoid #7 "Our risks are in our annual risk management plan."

I'm often asked by concerned senior executives why their risk management programs don't appear to be dynamic or why risks were realised that were not in their risk profile. When I ask how and where they store their key risks, the reply is sometimes in an annual risk

management plan. Or even worse, that the risks are Section X of their risk management policy documents. Neatly bound and placed on a shelf.

Placing risks into something endorsed once a year or into a policy document is guaranteed to lock them into a state of stasis and make them irrelevant to the actual management of risk on a day to day basis. In theory, risks should be updated every day. In practice, this may be aspirational but placing your risks in a form that prevents or discourages routine refresh doesn't help.

A question to ask in response to this factoid include:

- Is our organisation and environment really so static, that an annual update of our risks is appropriate?

Risk Management Factoid #8 "We have zero appetite for that risk"

If you are exposed to a risk, and you genuinely have zero appetite for it, then just stop doing whatever it is you are doing. A common example is "we have zero appetite for fraud risk", yet the organisation routinely spends money and lets contracts etc. What they mean to say is "we have zero appetite for fraud, if and when it is detected". Fraud control is a great example where getting the proportionality of controls is crucial. Expressing a realistic appetite for the risk is important in setting that.

As we reduce risk, the cost and impact of controls rises exponentially. Zero risk is unachievable and unaffordable, so let's stop saying we have zero appetite for it.

Questions to ask in response to this statement include:

- Are we really prepared to pay truly enormous and disproportionate amounts to reduce this risk so much?
- What opportunities and outcomes will we miss by minimising this risk so strongly?

Risk Management Factoid #9 "That's not a risk, we've got that under control"

So, you've got a big scary risk that you have (or think you have) well controlled. This might make it of low severity today. "So, let's take it out of our risk register."

Where is it going to go? Most likely into the sea of good intentions, in which case it will almost certainly be realised. It's a bit like taking your parachute off half-way down because it has slowed your descent.

High inherent severity but well controlled (in fact or fiction) risks are the most dangerous you are managing. They may have currently low severity (and be green) but they are critically dependent upon the controls that are thought to be in place. If the circumstances change and render the controls less effective or you've overestimated their effectiveness these become watermelons. Just because a risk might be under control today in no way stops it being a risk.

Questions to ask in response to this factoid include:

- What assurance can you provide that your controls are as effective as you think they are? Are they sustainable, well understood, holistic, resilient, timely, and assured or do they just happen to be working so far?
- Ok, so we've got the risk to green through lots of hard work, if we take it out of the risk register what will ensure that continues?

Risk Management Factoid #10 "I can't control all of that risk, it's not going in my risk register"

I'm often amazed at the salaries being paid to people who won't take ownership or stewardship of a risk because they or their business unit is only a part of it. Modern risks are almost never contained completely within a single organisational silo and are almost always shared across units, projects, organisations.

This is why I prefer the term risk steward to risk owner – to me it conveys the right expectations and accountabilities. No one ever really owns a risk, and it conveys the sense that "it is your fault if the risk you own is realised". This is usually not true. A risk steward is responsible for proactively monitoring the risk and communicating with the right people if things change. Reduced to a single sentence, it's as simple as that. If the risk is well analysed, controls and treatments implemented, the context monitored, and the residual risk accepted, there always remains the opportunity for the risk to be realised. That's why it's a risk.

Questions to ask in response to this factoid include:

- If you don't take lead on this risk, who is better placed?
- If no one steps-up to steward this risk, what's going to happen?

Summary

Although it's not included above, one of the most annoying things I hear is "that risk management concept has no value". It might sound out-of-place in an article bemoaning risk myths, but I believe there is never a single right way of managing risk.

If you genuinely think there is only one way to do 'risk management', you're in the firm grasp of the Dunning-Kruger effect and need to broaden your mind. There are quantitative methods and qualitative ones, COSO and ISO 31000, highly structured approaches and very fluid ones. There are additional concepts such as inherent risk, vulnerability, risk velocity, risk appetite, and tools such as dedicated risk information management systems. Each have their pros and cons but are none are inherently right, wrong or useless. Their utility and fitness for purpose in each circumstance is the conversation that needs to be had. We need to be equipped and prepared to constructively challenge the risk management factoids we hear, regardless of how confidently they are spouted.

First published 27 May 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 premium 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 Yutacar via Unsplash