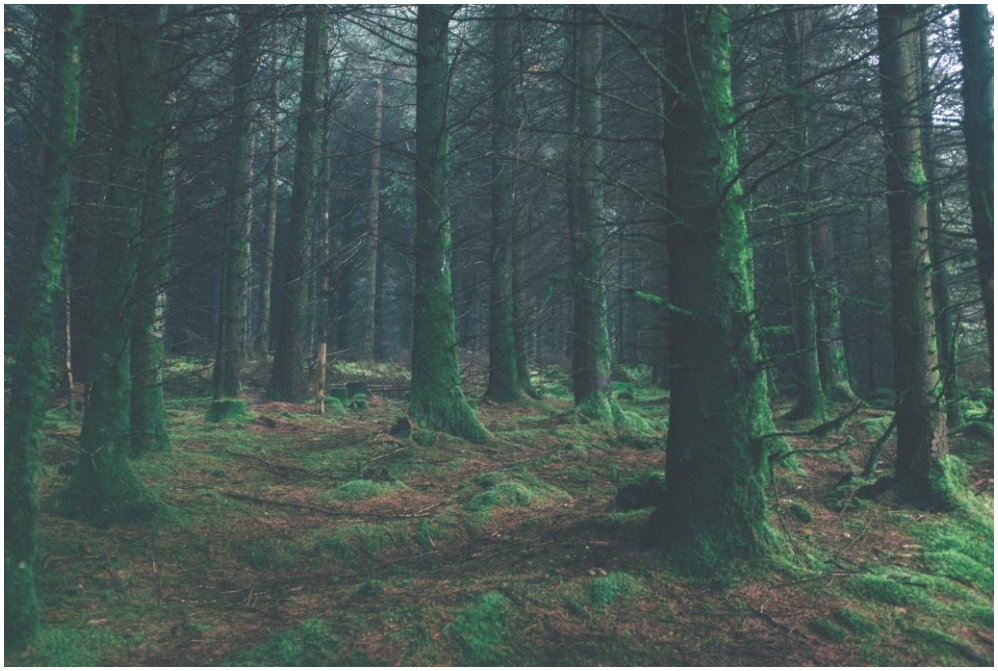
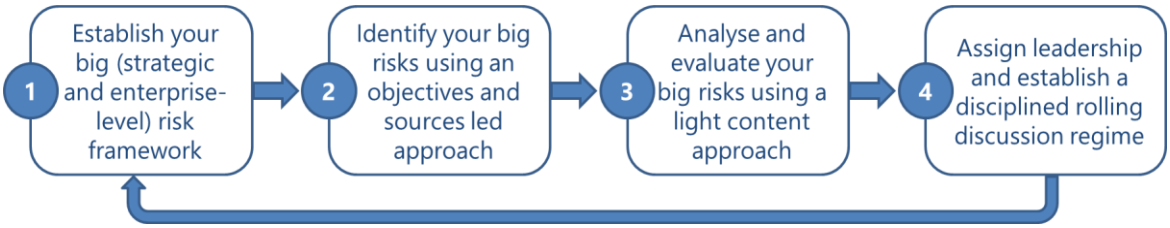


Big risk – Demystifying enterprise-level risk

Sometimes you need to see the trees, but sometimes you need to be able to look at the forest, and it shouldn't be so hard…

An arcane art has grown around the identification of 'big' or enterprise-level risk. Leadership teams are confused by the diverse natures of their big risks and can struggle to have a coherent management conversation about them. Complex processes have been developed to derive these risks, seemingly to provide 'science' or perhaps to justify billable consulting hours. Similarly, once organisations have identified their biggest risks, they don't know how to operationalise them, or worse simply put them aside until their next annual refresh. A simpler and more outcomes-focused approach is needed.

Although like everything in risk, there is no single right way to do it, I believe a practical four-step process can be applied to identifying and managing any organisation's big risks.

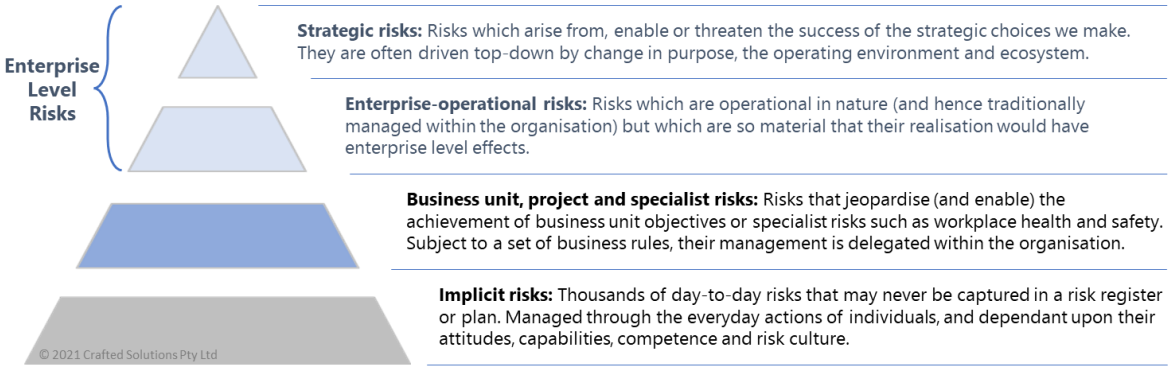


Throughout this process it is important to remember that risk is the effect of uncertainty on objectives. Accordingly, this approach aims to identify and help manage the big uncertainties to an organisation being successful. It is not a compliance exercise documenting long lists of anxieties to appease your auditors.

Step 1. Establishing your big risk framework – acknowledging the differing natures of big risk

Different terms are used to describe big risk. They are sometimes referred to as 'strategic' and sometimes as 'enterprise'. Big risks can be both or either - they are simply the big risks and uncertainties that need hands-on management and/or visibility by the organisation's most senior team.

Modern complex organisations manage many risks. They are commonly arranged as systems of risk profiles (sets of risks sometimes stored in a risk register), typically in some form of pyramid or hierarchy. The top two layers are enterprise level or 'big risk'. The lower two layers are managed within the organisation, either explicitly through structured processes or through the everyday decision making of staff at all levels.



For most organisations, their biggest risks sit on a spectrum between those which are truly 'strategic' and those which are 'enterprise-operational'.

- The Oxford Language Dictionary defines 'strategic' as an adjective meaning "relating to the identification of long-term or overall aims and interests and the means of achieving them." Strategic risks are those that create uncertainty in your ability to determine and achieve these 'big goals' and should influence the strategic choices you make.
- Enterprise-operational risks are more focused on activity within the organisation, but where the consequences of getting it wrong are so material they could have enterprise-level effects. Some might call these big 'operating risks' or risks to the operational execution of the strategic plan.

The difference is important (noting it is shades of grey, not black and white), as different conversations and management strategies are required. One type is not necessarily more important than the other, but understanding that your big risks sit on that spectrum and can't all be managed in the same way helps tailor an approach to the management of each. For example, the executive or Board conversation on managing risk in a fundamental transformation of your sales channels will be a very different one to managing internal fraud risks.

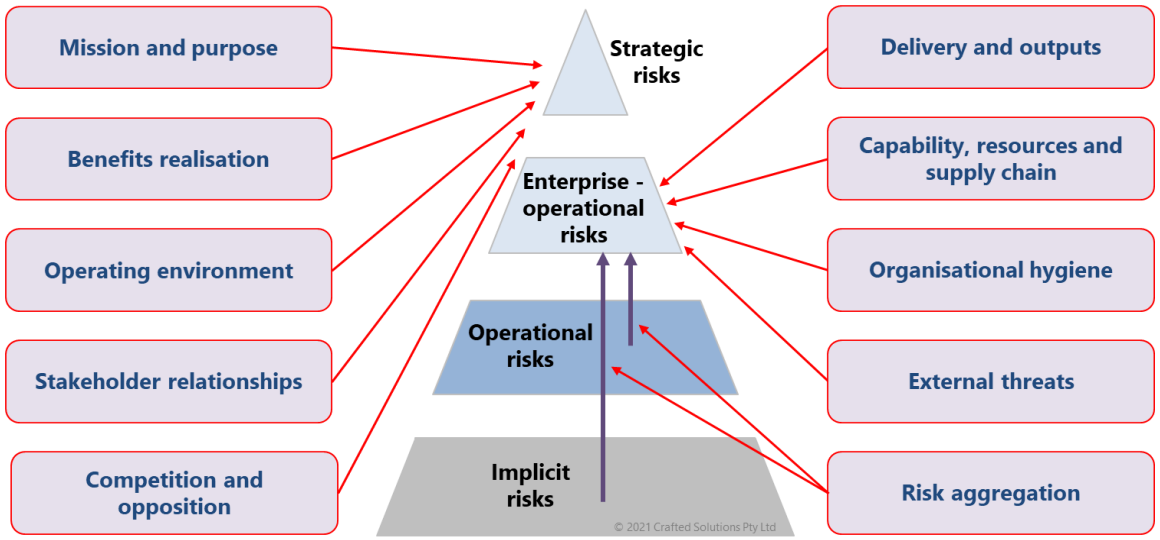
Strategic risks: Risks which arise from, or threaten the success of, the strategic choices we make. They are often driven by change in purpose, the operating environment and ecosystem.	• Tightly linked to strategic priorities, often with significant potential upside. • Often quite differentiated for each organisation • Primarily derived top down • Future focused and considers key disruptors • Can be data light, discussion heavy • Will flex with the priorities of the time and be responsive to the operating environment and ecosystem • Complex **Senior Leadership Team's Primary Role:** Discussion, debate, and strategic choices.
Enterprise-Operational risks: Operating or operational risks of the type normally managed within the organisation, but so material that their realisation would have enterprise level effects.	• Often driven by implicit or unstated objectives, for example safety and security • Can be enduring and often common with similar risks in like organisations • Sometimes the bottom-up aggregation of operational risk across the organisation • Usually broadly relevant to all staff • Valuably informed by analytics and comprehensive reporting • More amenable to management through rules based systems • Complicated **Senior Leadership Team's Primary Role:** Resourcing, empowering, seeking assurance, rule-setting, and decision making by exception.

Step 2. Identifying your big risks

Like any discussion of risk, the starting point should be objectives – "what does success look like to the people who matter?" Any mention of risk as a stand-alone list of bad things that can happen in isolation is inevitably an exercise in anxiety management or catastrophisation. The identification of big risk relies on a clear understanding of success – both to you and to the people who matter. These are then compared to a set of sources of risk and uncertainty.[1] Big risk lies at their intersection.

[1] Many different terms are used for sources of risk – threats, vulnerabilities, opportunities, context, uncertainties or vectors. I will use the term in its most general sense.

Although there are many ways of slicing the pie, I see big risk emerging from 10 main sources. The diagram below illustrates these 10 sources and their likely primary contribution to your strategic and enterprise-operational risks.



The alignment of these risk sources against strategic or enterprise-operational is of course not absolute. It will depend upon what you consider a 'strategic' issue or choice. For example, although aligned against the enterprise-operational level, resourcing and supply chain resilience is an area where some very strategic choices can and need to be made. The important thing is that they are all considered in some way.

Considering each in turn helps overcome the bias of picking the 'usual suspects' or the worry of the day. A Harvard Business Review article noted that many risk managers in organisations spent over 50% of their time focusing on legal compliance and financial reporting risks, when these were only responsible for 5% of enterprise-level risk realisations.[2]

So, having identified what success is for your organisation, how do you then test these against the sources? Examples of some of the questions I ask follow:

1. Mission and purpose

Changes, ambiguity or inconsistent interpretations of an organisation's mission and purpose can generate big risk. If an organisation's purpose is contested it will create inherent uncertainty in the ability to achieve that outcome in the eyes of the people who matter. Similarly, how well is the organisation's purpose understood and core to your people's priorities and values?

As I've already noted, risk should always be anchored to objectives. If the objectives are unclear or contested, it leads to the risk that we are fighting in the wrong contest or for an unwanted prize. It creates risk about what we thought were our big risks! A bit like training your whole life to be a power weightlifter only to find you've been entered into a running marathon and will be judged on that basis.

[2] Harvard Business Review, How to Live with Risks, July–August 2015.

2. Benefits realisation

A great failing in risk management is focusing solely on outputs and neglecting outcomes. I refer to it as the "we built it, but nobody came" risk. We manage risks derived from too narrowly defined measures of success instead of the ultimate aim.

Benefits realisation risks are often complex and shared. The team focused on building the stadium may argue they can't be held responsible if no one wants to come to the games. But collectively somebody has to, and it might require stepping the maturity of the discussion on shared risk up a notch.

Questions to ask include:

- Do we fully understand the outcomes we seek to contribute to? Is there a risk that despite what we do, it won't make a difference in practice?
- Do we understand how and why (specifically) our work is valued or not? Can we measure outcomes or only outputs?
- Are there things that we cannot control that could stop our outputs from generating those outcomes?

3. Operating environment

Big risk can emerge from changes in your operating environment or ecosystem – either now or anticipated. The well-known PESTLE mnemonic is a useful checklist for considering environmental factors that might lead to big risk for an organisation. Changes can be either gradual or sudden.

Political	What are the key political drivers of relevance – globally, nationally, State or Territory, and locally? Are there new or possible regulatory obligations or changing policy positions of significant relevance?
Economic	What are the most important economic factors - funding mechanisms and streams, business and enterprise directives, internal funding models, budgetary restrictions, income generation or cost reduction targets?
Social	What are the main societal and cultural drivers or changes? This includes general lifestyle changes, changes in populations, distributions and demographics, and evolving community expectations. How is the media and social media influencing this?
Technological	Will any emerging technology enablers or disruptors impact on how we work or what we produce? For example, will we, or any of our key partners, stakeholders or clients be using technologies different from today?
Legal	Is there any current or impending legislation that will impact us, our stakeholders or our responsibilities? Changing interpretations of law?
Environmental	Are there natural and built environmental considerations, locally or further afield? How will climate change affect us and those we share risk with?

Once the PESTLE elements have been considered, the final questions to ask in this category are "Are we generally good at change? Do we have mature mechanisms in place to anticipate and respond to change in our operating environment, regardless of its nature?" If the answer is no, this is likely to be a broad contributor to your big risks.

4. Stakeholder relationships

Damage to important stakeholder relationships is a common consequence of the realisation of big risk. Sometimes though, those relationships are so critical that their health needs to be managed as a big risk in its own right.

Questions to ask include:

- Who are our most critical stakeholders? Are we at risk of losing the support or confidence of those we rely on?
- Are there impediments in our ability to communicate effectively with key stakeholders, or understand what matters most to them?

5. Competition and opposition

Sometimes thought to be only a private sector or commercial concern, all organisations face uncertainty created by competing and opposing interests. Organisations, both public and private, exist because someone thinks you can do the job better than others - it's just a bit more direct and immediate in the private sector.

Questions to ask include:

- Do we face competition now? Could new entrants be attracted into our market? Are we a merger or acquisition target?
- Could either the outcomes or outputs we generate be delivered by someone else or in a different way (in reality or perception)?
- Is there a chance that the people who buy or pay for our work will no longer view it as a good investment?
- Are there stakeholders who are actively or passively adversarial to us or our goals? Are they influential or potentially influential?

6. Delivery and outputs

Accepting the organisation's outputs for what they are, what are the big uncertainties associated with being able to generate and deliver them?

Questions to ask include:

- What are our key processes, outputs and products? Are any of these at jeopardy of failure? Can we maintain their required quality and quantity?
- What activities do we undertake that inherently contain risk? Where is our work hazardous or experimental?
- Is there a risk of negative outcomes or undesired by-products from these processes or outputs?

7. Capability, resources and supply chain

Most organisations are reliant on specialised internal capabilities or external providers as key inputs to their work. These capabilities, supporters or supply chains may be vulnerable to compromise or disruption. Questions to ask include:

- What are our key inputs and capabilities - supply chain, resources, enablers, people, information and data, funding or appropriations, systems, or infrastructure? Which contribute to our core outputs – both most importantly and most urgently?

- Are any of these key inputs uncertain, scarce, single-sourced or otherwise vulnerable? Do we have alternative plans? How effectively do we monitor their status, quality, prospects and potentially alternative plans?
- If any were to become unavailable to us, how well can we flex, adapt or evolve our how we work?

8. Organisational hygiene

Organisational hygiene is a term I use to refer to whether an organisation is able to meet its 'licence to play' requirements. These include operating safely, legally, securely, inclusively, ethically, sustainably and in accordance with applicable policies, regulations and laws.

Questions to ask:

- Do we deeply understand the 'licence to play' requirements applicable to us and if they change? Do they differ across our organisation?
- How do we know we are appropriately compliant? What assurance do we have and is accountability clear?
- Are these behaviours embedded in our culture or simply rules to be followed?
- Is our organisation meant to be the exemplar of something that we simply cannot afford to get wrong? For example, if our organisation is an anti-corruption watchdog, we better manage our own internal corruption or integrity risk with a laser focus.

9. External risks

Robert Kaplan and Anette Mikes referred to 'external risks'. "Some risks arise from events outside the [organisation] and are beyond its influence or control. Sources of these risks include natural and political disasters and major macroeconomic shifts. External risks require yet another approach. Because [organisations] cannot prevent such events from occurring, their management must focus on identification (they tend to be obvious in hindsight) and mitigation of their impact."[3]

Other examples of external risks include terrorism, neighbouring industrial disasters, civil disorder or breakdown, war, pandemic, or systemic infrastructure collapse. In considering these risks, often geographic or national factors are very important. Do we have operations, interests or dependencies overseas that might be vulnerable to some of these threats?

Individual external risks can sometimes be seen as too unlikely to warrant attention in isolation. To overcome this, external risks are best managed by considering classes of risks with common potential consequences. For example, having well-conceived, tested and exercised building evacuation protocols is a mitigant for many dozens of potential external threats to a building or facility.

10. Aggregation of risk

Finally, it is important to capture any risks lurking within the organisation that need consideration for elevation to an enterprise level. These could be individual risks or the aggregation of many small but similar risks in the lower tiers of your risk pyramid. In these lower tiers there could be dozens, hundreds or thousands of diverse risks being managed. It is critically important that someone has the role of sifting these signals from this noise.

[3] Robert Kaplan and Anette Mikes, "Managing Risks: A New Framework", Harvard Business Review, June 2012.

If a large proportion of your mid-tier managers are dealing with the same uncertainty, it may be a candidate for elevation as a big risk. Even if these smaller risks are individually all only of only modest severity, the cumulative uncertainty they represent (particularly if they have common causes, triggers or interdependencies) could be significant. Where does risk need to be managed in aggregate at an enterprise level?

Compiling a manageable big risk list

Once objectives and sources of risk have been agreed and compared to form a starting list of big risks, the secret is then distilling these down into a number actively manageable by the executive leadership team. I refer to them as the 'top 10' for a reason. Interesting, but otherwise narrower risks can be delegated for management into the organisation and subject to a set of business rules and reporting requirements. Push them down the 'layers'.

Step 3 – Analysing and evaluating your big risks

Again, a lot of mythology and calcified process governs how risk is often analysed and evaluated. Likelihood and consequence tables and severity ('heatmap') matrices unfortunately have become dominant. I believe these approaches to be of dubious value at the best of times, but for big risk I see them add baggage and process without adding any real value.

Determining a point-value of the likelihood of a big risk occurring through a table of nominal percentages adds little to the discussion. It is considering and managing the sources, causes, potential triggers and likely consequences of the risks that allows you to make decisions about them. i.e. actually discussing and considering the means and pathways by which the risk could be realised and the likely effectiveness of controls and proposed treatments.

Risks at this level should also be managed as 'when' not 'if', either individually or as classes of event. For example, like many Australians, I live in a bushfire prone area and in recent years a fire burnt down several of my near neighbours. Frankly, I am not interested in the % probability of this reoccurring in the next few years. Ultimately, it is of sufficient likelihood and potential materiality that I am going put in place a strong set of proportionate preventative (mowing and firehoses), detective (fire notification app) and mitigative (insurance and off-site data backup) controls in place.

At the top table, more so than anywhere, you need streamlined and clean approaches that support discussion and decision making, not exhaustive analysis and compliance. This is particularly the case with your strategic risks. The key questions to ask and to document for each of your big risks are:[4]

1. **What are the possible consequences?** Which of the objectives or measures of success (identified earlier) are uncertain because of this risk? What's the prize we stand to lose by accepting or rejecting this risk? The potential for cascading consequences (risks triggering other risks) should be particularly noted.

2. **Why is this a big risk?** What contextual factors, sources or conditions cause this risk to exist, make it as severe as it is, or could trigger it? What do we know, assume, or not know, about the sources of risk that concerned us in the first place?

3. **What is being done now to manage it and how effective are these controls today?** What preventative, detective or mitigative controls or actions are in place? This includes controls we

[4] Refer to my article "*Risk Management Without Matrices*" for an expansion on this line of questioning.

have implemented as well as those applied by others on our behalf. How effective are they in practice?

4. **How concerning or acceptable is the risk today?** Many risks cannot be completely eliminated without the organisation stopping what it does. But, how comfortable are we that the objectives in jeopardy are sufficiently achievable? Is it within our appetite? Considered in context, if this risk were realised one day how would we feel looking back at how it was being managed?

5. **What are we going to do about it?** Rather than just accepting that high risk is bad and low risk is good, every risk deserves its own treatment strategy. What are we going to do differently tomorrow as a result of this exercise?

For those familiar with the concept (or with access to an Internet search engine), I highly recommend the simplified 'bow-tie' risk visualisation as a great way to structure and communicate the analysis above.

So far, I have been deliberately and perhaps provocatively light on the risk analysis process. In some environments and for some organisations, you will need to conduct perhaps quite detailed and quantitative analysis of your big risks, including your strategic ones. This should be built into your approach as needs require.

Step 4 – Managing your big risks

Having invested in steps 1 to 3, too often, the big risks are then proudly printed in a corporate or strategic plan, reported to a board or committee, and then quietly parked until their next annual review. If we've agreed that these are the few biggest uncertainties to being successful, they should be receiving regular, disciplined and structured attention.

Big risks should be discussed each in detail on a rolling basis – one or two every executive leadership team meeting or so. This is preferable to scheduling the review of all the big risks in a single session which often becomes a rushed compliance exercise.

How each risk is best updated and discussed differs depending upon where the risk is on the strategic/enterprise-operational spectrum. More strategic risks will suit discussions and debates, whereas more enterprise-operational risks will benefit from structured briefings, expert reports and a more traditional governance focus.

To lead the management of each big risk, I recommend the assignment of a senior steward for each. In some cases, a given officer will be the logical senior steward for a risk by right of their portfolio responsibilities, in others someone might need to step up and steward a broad enterprise uncertainty which may have no natural single owner. Their role is to actively lead the monitoring of the risk, oversee its maintenance in the enterprise-level risk profile/s, and to brief the risk at each leadership conversation.

Summary

The process for identifying and managing your biggest risks should be simple and practical. A competent leadership team clearly identifying what success looks like and then comparing this to the main sources of big risk will likely identify your 'top ten'.

Acknowledging the different natures of big risk, starting with success, keeping the analysis simple and outcomes-focused, and having a regular structured discussion and reporting regime is the key.

v1.0, originally published in Lexus Nexus – "Risk Management Today", Vol 31 No 9 November 2021.

Sal Sidoti changes the way people and organisations think about risk. He has over 30 years' experience working within and advising 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. Outcomes not templates, approaches that go beyond cut-and-paste compliance and death by spreadsheet. Sal is the Director and Principal Consultant of Crafted Solutions Pty Ltd and is home based near Canberra, Australia.

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

Title illustration courtesy of Vital Sinkevich via Unsplash

