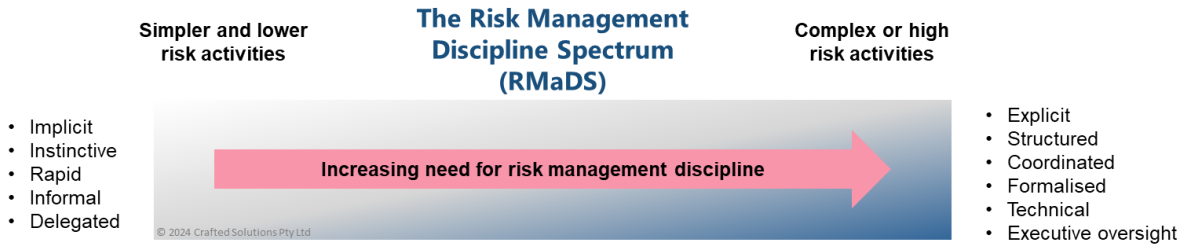
Risk management – more than 50 shades of grey

But how much discipline do you need?

Anyone whose worked in risk management for more than a week or two will have heard "I don't have time to do this risk management rubbish. It's too time consuming, too complex, too bureaucratic, or doesn't add any value!" You may have expressed the same frustration yourself.

There are many reasons to hold this view, some reasonable and some not so much. But one of them is a perception (rightly or wrongly) that the risk management approach is not proportionate to the situation or outcomes being sought.

The need for discipline, rigour, and process in risk management exists on a spectrum. In some cases, it needs to be rapid, intuitive and efficient. In others, its needs to be considered, coordinated, and potentially sophisticated. I call this the Risk Management Discipline Spectrum (RMaDS). The risk management approach you take at different points on the RMaDS should vary in both scale and nature.



There is a spectrum of need, and a spectrum of tools and concepts that can be applied

Operating at the left of the spectrum, the onus is largely delegated to the individual, and the outcome will depend heavily on their innate ability to manage risk. They can bring their experience and judgement to bear and there is significant opportunity for both entrepreneurial success and careless failure.

At the right, the organisation directs and controls the management of risk.

There is extensive use of frameworks and process. These can be onerous and can take time to complete, but they are repeatable, consistent and defensible.

Most of the time, you will be between the two extremes, one of the shades of grey. But I often see organisations or programs operating at the wrong place on the spectrum, either loading themselves with unnecessary bureaucracy, or being 'Santa's little workshop' – well-meaning elves happily making teddy-bears and toy trains in the face of daunting and complex risk.

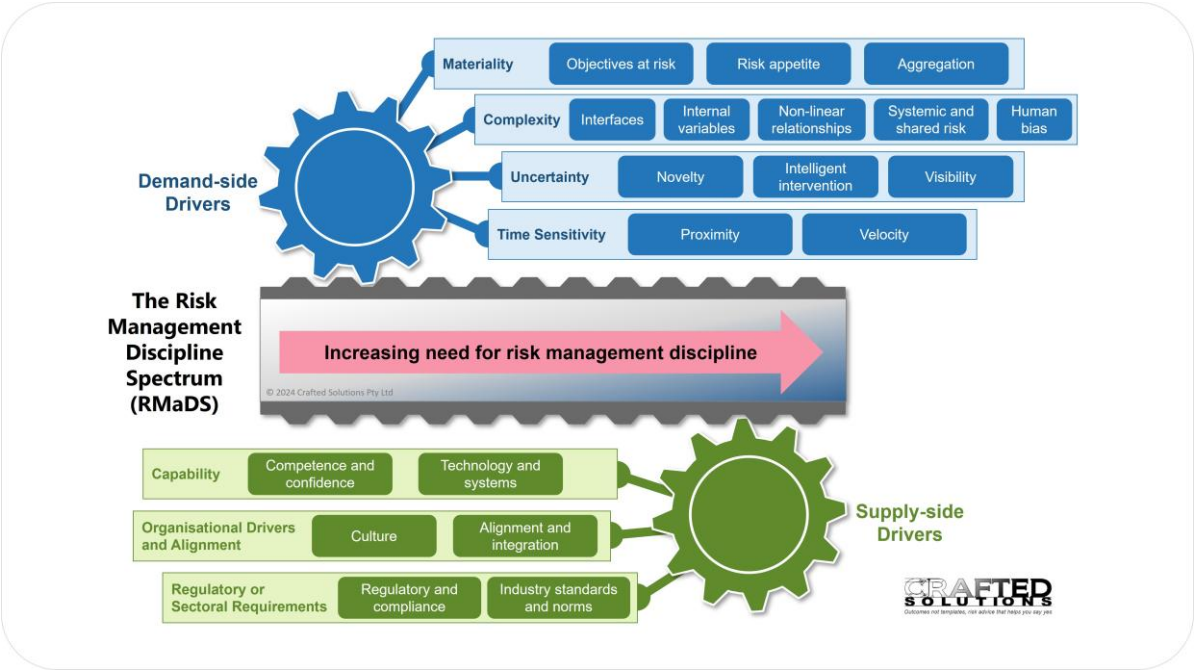
There are parallels here to the attributes and limitations of the System 1 (fast, intuitive, and emotional) and System 2 (slower, more deliberate, and more logical) ways of thinking described in Daniel Kahneman's book "*Thinking, Fast and Slow".* In this essential reference for any risk professional, Kahneman explores the contrasts, benefits and pitfalls of both systems in great detail.[1]

How much risk management discipline do you need?

Applying an adequate level of risk management discipline is essential for maintaining organisational resilience, protecting assets, ensuring compliance, and fostering trust among stakeholders. It allows organisations to anticipate, assess, and respond to risks effectively. Not going too far though is essential to efficiency, innovation, agility, uptake, and seizing value. The best risk systems seek to combine both, but particularly for novice risk managers this isn't always straightforward.

So, there is value in thinking carefully about where on the RMaDS you should be operating in any given situation. But what factors do you consider when doing this? And in a defensible and repeatable way?

Illustrated below, you need to consider both "demand-side" and "supply-side" drivers.



[1] *Sadly, Professor Kahneman passed away in March 2024.*

Demand-side drivers

Demand-side drivers are the characteristics of the situation or risk system you are dealing with that require you to apply more or less risk management rigour and sophistication. Key demand-side factors you should consider include materiality, complexity, uncertainty, and time sensitivity.

Materiality

Materiality is a measure of the potential consequences should you get the risk decision right or wrong.

Materiality can be determined objectively (such as in a bank considering a new product class) or subjectively. Regardless, three main elements contribute to the potential materiality of any risk system – the importance of the objectives at risk, the risk appetite of the organisation, and the potential for aggregation of risk in the system. The concerns and appetites of stakeholders should also be considered.

- **Objectives.** Risk management is all about achieving objectives – both value creation (things you want to get right) and value preservation (things you don't want to get wrong). The importance of the objectives at risk (both to you and to the people who matter) should be the primary determinant of the materiality of any set of risks.
- **Appetite or non-negotiables.** Some dimensions of consequence are unique to a particular organisation or situation. They are areas of particularly low risk appetite (ours or important stakeholders) and sometimes referred to as 'trophy risks'. They are risks that might be minor for most organisations, but for us, getting them right is fundamental to our 'licence to play'.
- **Potential for aggregation.** Aggregation asks what the true consequence would be should several risks occur at once or in quick succession. It helps understand the actual risk exposure for all or a part of an organisation or project and can be more than just adding together your individual risks. There is the chance that if two or more risks are realised simultaneously or in brief period of time, that the consequences might be multiplied (i.e. more than the simple sum) or be unacceptably damaging. Feedback loops and failure cascades can also greatly increase the potential materiality of any risk system.

Complexity

Complexity is a measure of the number and nature of components within a system and its internal and external relationships and interconnections. The more complex the risk system or context, the more sophisticated your risk assessment approaches may need to be.

- **Interfaces and interconnectedness.** Risks that are interconnected or have cascading effects with other risks or systems may need more comprehensive assessment to understand their broader implications. Similarly, risk systems with many stakeholders are likely to require approaches that can consider often-conflicting perspectives and expectations.

- **Internal variables and complexity.** Risks involving multiple variables, factors, or dimensions are often complex because of the interactions and dependencies among these elements. This is particularly the case with risk systems that are internally highly diverse. Analysing the relationships between variables and assessing their combined impact can be intricate. Think about assessing risks on the apron of a modern commercial airport. There are aircraft, refuelling trucks, passenger buses, security services, moving infrastructure and even sometimes wild animals. It is a complex risk environment with high internal diversity.
- **Nonlinear Relationships.** Risks that exhibit nonlinear relationships between cause and effect can be complex and unpredictable and require more sophisticated risk analysis approaches. In such cases, small changes in one variable may lead to disproportionately large or unexpected outcomes, making it challenging to predict the overall impact accurately. Examples of non-linear relationships include threshold effects (e.g. ice sheet melting), feedback loops (e.g. population/resource depletion in wildlife systems), or chaotic systems (e.g. weather patterns).
- **Systemic and shared risk.** Risks that have the potential to affect entire systems or industries, rather than isolated components, can be complex because of their systemic nature. These risks may involve interactions between different stakeholders, institutions, or markets, amplifying their complexity. Similarly, risks that transcend organisational or geographic boundaries can be complex because they may involve collaboration among multiple stakeholders with diverse interests and perspectives.
- **Potential for human bias**. People can be bad at making good risk decisions and are susceptible to a diverse range of cognitive biases. Additional risk management discipline may be required in risk systems particularly vulnerable to these biases. An example is a person making investment decisions who is being swayed by confirmation bias[2] and overlooking risk in their preferred investment choice. They may need more robust financial risk advice!

Uncertainty

Uncertainty is the predictability or novelty of the risk system or how familiar you are with it. Although sometimes viewed as an element of complexity, I've called it out separately as it is an inherent determinant of risk. Risks with high levels of uncertainty, even if they are not particularly complex, may require more rigorous assessment techniques.

- **Novelty.** Novel circumstances, or situations you are unfamiliar with can require more rigorous risk decision making or scrutiny. Conversely, risks that have occurred in the past or have precedent in similar contexts may require less rigorous assessment if there is existing knowledge and experience to draw upon. 'Emerging risks' may exhibit significant novelty.

[2] Where the risk decision maker seeks out information that confirms their existing beliefs and ignores evidence of undesirable risk in that choice.

- **Intelligent intervention.** Humans (or other intelligent actors) always add an element of uncertainty to any risk situation. People are unpredictable and may also seek to actively circumvent controls in place. From an engineering perspective, the risk of a bolt failing is relatively determinable, but if someone decides to remove the bolt…
- **Visibility or understanding of the system.** The extent to which you understand how a system works (regardless of its complexity) or can see into it will influence your perception of uncertainty within it. A fair coin toss is well understood by most people - there are only two possible "consequences" – heads or tails, and the likelihood of each is 50%. So, although the potential result of each individual throw is unknown, the uncertainty in the system is relatively transparent.

Time sensitivity

Time sensitivity is a measure of the volatility of the situation and how rapidly the risks might be realised or change. Although the terms are not authoritatively defined, the proximity and velocity of the risks in the system you are considering are important to consider:

- **Proximity**. The proximity of a risk refers to how soon the risk/s could be realised. Generally, proximate or near risks need rapid assessment. This can constrain the risk management rigour you can apply unless the risks are commonly experienced and established rapid assessment methodologies are in place.
- **Velocity.** Velocity is a measure of how dynamic the risk system is and how quickly the risk/s could change. Rapidly evolving risks generally need more sophisticated risk management systems to ensure that assessments and controls are current and can evolve as quickly as the risks themselves.

Supply-side drivers

In addition to these demand-side drivers, the characteristics of the organisation or ecosystem you are working within also determines how much risk management discipline you can sensibly or practically apply. These supply-side factors can be independent of the characteristics of the risk problem you are dealing with.

Not considering 'supply-side' factors can lead to risk management approaches that are theoretically sound, but unimplementable or unsustainable. Key supply-side drivers you should consider include the available risk management capability, organisational drivers and alignment, and regulatory or sectoral requirements. You should be cautious though as to how much you allow supply-side drivers to 'water down' the appropriate risk approach and be alert to when it becomes excuse making. This requires professional judgement.

Capability

The availability of resources, including expertise and technology, influences an organisation's capacity to deploy and maintain (this is often more important than the initial build) risk management discipline.

- **Competence and confidence.** The capability of an organisation's people, including the risk team, is an important determinant of how much and what nature of risk

management sophistication can be applied. This applies at a background level as well as considering any specific requirements for expertise a particular nature of risk might have.

- **Technology and systems.** An organisation's technology and systems play a crucial role in shaping its ability to implement effective risk management, in particular sophisticated risk management analytics and workflows.

In addition to assessing the current level of capability, you may also consider implementing a level of risk management discipline to deliberately foster and enhance that maturity.

Organisational drivers and alignment

Each organisation is unique. Carefully consider the environment you are working within and how you can maximise your chances of successful implementation and uptake.

- **Organisational culture.** An organisation's culture and sense of "the way we do things around here" affects its appetite for risk management discipline. Some organisational cultures are comfortable with rigour, processes and governance, whereas others consider this to be largely bureaucratic nonsense.
- **Alignment and integration.** The management of risk is most effective when embedded and integrated into other decision-making processes. If your system has well-functioning planning mechanisms in place there is value in aligning with them, including how much rigour and sophistication you apply. Consider past successful approaches in other areas for valuable lessons.

Regulatory or Sectoral Requirements

Besides considering our own organisation, the ecosystem in which it operates can also affect the appropriate level of risk management discipline.

- **Regulatory and compliance requirements.** Organisations in highly regulated sectors may need more robust risk management systems to remain compliant. Likewise, risks that are subject to specific regulatory or compliance requirements may require more rigorous assessment to ensure adherence to sometimes quite specifically defined standards.
- **Industry standards, best practices and expected norms.** Failing to align with industry standards or accepted good practice can lead to criticism or perceptions of misalignment, regardless of how proportionate you might feel your approaches are. It can be important to be seen to be doing the right thing in a sufficiently robust way.

Summary

We manage risk between extremes—either boldly improvising or mechanically overthinking. Both of these extremes are occasionally warranted, but most of the time we need to be at a shade of grey.

To achieve this successfully, it is important to think deliberately and pragmatically about how much risk management rigour is needed in any given situation. Force-fitting a risk

management approach that isn't proportionate will ensure you are 'trying to solve the wrong problem' regardless of the methods you adopt.

Everyone needs a little discipline once in a while, the trick is ensuring it isn't too hard or too soft.

First published April 2024. This version updated April 2025.

Sal Sidoti changes how people and organisations think about risk. He has over 35 years' experience working with public and private sector organisations across Australia and further afield. Sal designs and implements tailored risk arrangements 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 and is home based near Canberra, Australia.

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

Title image courtesy of Spencer Arquimedes via Unsplash.

