



★ S2 – Issue Four, Assess the ‘Would’ not the ‘Could’

Series Two: Improving Decision Quality in Uncertain Environments

Most organisations believe they are being prudent when they overestimate risk. Few recognise they may also be making poorer commercial decisions.

Several years ago, I estimated the expected annual losses across the operational risks within a medium-sized Australian financial services organisation. To reduce duplication, I first aggregated individual risks into broader operational risk categories before estimating their expected losses.

Even then, the framework suggested annual losses should be more than ten times the organisation's actual loss experience. Risk assessment has never been a precise science, but the magnitude of the overstatement was striking.

The conclusion was difficult to ignore. We were consistently assessing what **could** happen rather than what we **would** reasonably expect to happen.

That distinction matters because every risk assessment influences where organisations invest time, money and management attention. If the assessment is materially overstated, the investment decision will be too.

Good risk assessments are not about predicting the future. They are about improving today's decisions.

Core Insight

When people assess risk exposure, they naturally gravitate towards the worst conceivable outcome.

Psychologists refer to this as the availability bias—we are drawn to memorable, high-impact events. In business, we reinforce this behaviour through discussions about Black Swan events, unknown unknowns and worst-case scenarios.

These conversations are essential for resilience planning. They are far less useful for estimating routine risk exposure. Likelihood does not feature in those discussions, so they should not become the anchor for routine risk assessments.

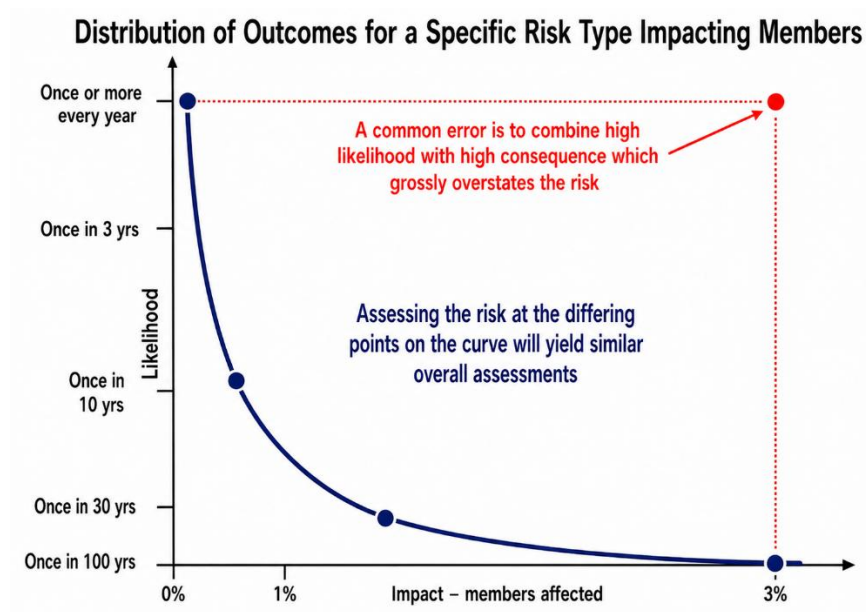
Routine risk assessments should estimate what would reasonably be expected if a risk materialised, not the most extreme outcome theoretically possible.

Every risk should be thought of as a distribution of possible outcomes rather than a single event.

Before any assessment can occur, the risk itself must be tightly defined. Broad descriptions such as "cyber risk" or "technology failure" encompass many different events with very different outcome distributions, making consistent assessment impossible.

Once defined it is likely some risk incidents may occur frequently with relatively modest impacts. Other more severe outcomes may also be possible, however, these would be expected to occur rarely. The challenge is not recognising that a range of outcomes is possible—it is deciding where on that distribution we should anchor our assessment.

The illustration below demonstrates the concept.



Each blue point represents a commercially defensible assessment point because the likelihood and consequence remain aligned (the points away from likelihood or impact extremes will be more reliable). The red point does not. This is perhaps the most common assessment error made in operational risk frameworks. It combines the likelihood of a relatively common event with the consequence of an exceptionally rare event, grossly overstating the actual risk exposure.

That mismatch is surprisingly common.

It systematically inflates risk assessments and explains why so many enterprise risk heat maps become dominated by High or Extreme risks. Once everything is assessed as critical, very little can be genuinely prioritised.

Risk assessments should drive commercial resource allocation.

Every risk assessment is also an investment decision. If the expected exposure is overstated, the implied investment required to address that exposure also becomes overstated.

Viewed commercially, organisations should generally be prepared to invest up to the expected loss of a risk to eliminate it. Beyond that point, the economics increasingly favour accepting some residual exposure.

Internal incident and write-off history, external incidents, industry loss databases and emerging trends all provide valuable reference points that help risk owners anchor their assessments in evidence rather than speculation. The most valuable question a risk function can ask is: "What assumptions underpin this assessment?"

Risk assessments should not be anchored on insurable limits as these are based on extreme very low probability events.

Implications for Executives

For Boards and Executive teams, the implications are significant. Risk assessments exist to improve commercial decisions, not simply to produce risk ratings.

When risks are systematically overstated, the implied investment required to mitigate them also increases. Organisations become more conservative than necessary, invest heavily in lower-value controls and lose visibility of the risks that genuinely deserve management attention.

Boards should therefore be cautious of risk frameworks where almost every material risk is assessed as High or Extreme. That is often evidence that the assessment process is failing to differentiate, rather than evidence that the organisation is uniquely risky.

Viewed collectively, an enterprise risk framework contains a portfolio of risks requiring investment to mitigate. When we assess them on a **would expect** rather than a **could expect** basis their exposures are anchored as close as possible to reality. Scarce resources can then be directed where they have the greatest impact.

Ultimately, the purpose of risk assessment is not to identify the most extreme future. It is to help management allocate finite resources to the future that is most likely to unfold.

Practical Takeaways

When reviewing a material risk assessment, ask five simple questions.

1. Is the risk clearly defined?

Broad risk categories almost always produce inconsistent assessments because they contain multiple outcome distributions.

2. Are we assessing what would reasonably happen, or what could theoretically happen?

Routine risk assessments should be anchored in expected outcomes rather than exceptional tail events.

3. Are likelihood and consequence aligned?

Avoid combining the likelihood of a common event with the consequence of an exceptionally rare outcome.

4. What evidence supports the assessment?

Historical losses, industry experience and realistic management responses should inform judgement wherever possible.

5. Does this assessment change how we should allocate finite resources?

The purpose of a risk assessment is not to generate ratings. It is to help management allocate finite resources where they will reduce the greatest amount of expected loss.

Commercial risk assessment should estimate the probable. Resilience planning should prepare for the possible. Confusing the two inevitably leads to poorer decisions.