How the hell did we get here?!

(and how do we get back to where we started?)

Grant Purdy, Director Sufficient Certainty Pty Ltd)

Summary

Mankind has always sought to understand the uncertainty the future brings so that he or she can make decisions that lead to good outcomes. However, it is only in the last 20 years or so that what is commonly called 'risk management' has in many ways become significantly divorced from making better decisions and has become much more self-serving. To some, to demonstrate you are managing risk well you must produce artefacts of some process including lists of 'risks', rather that actually showing you have the capability and correct motivation to make better decisions in the face of uncertainty.

One thing that has remained through time, is that what the term 'risk' (and therefore other terms with that root) means, varies significantly between people. While it is surely one of the most commonly used words, which many regard as 'useful', there is no agreed definition, even among experts. Even International Standards contain over 50 different definitions!

In the 1990's learned experts of the Society of Risk Analysis spent four years trying to define what 'risk' is – and eventually gave up! Then, while a technical committee writing the world's only global standard on risk and how it should be managed did arrive at a reasonable definition of 'risk' in terms of a property of an organisation, it studiously avoided defining what 'risks' are.

Nevertheless, the term 'risk' is used extensively by everyone and especially by those who draft legislation, work in the media and seek to enforce statutes and litigate or defend us in legal arenas – largely without any consistency or clarity of meaning.

Typically, when you ask people what 'risk' means (as I have during training courses for over 40 years), the normal response is that, of course, everyone knows what it means. However, when you press them for a definition, invariably, you get as many answers as the people present.

One of the unfortunate consequences of a general willingness to get everyone involved in 'managing risk' (often, it seems by those new to the subject and who have no previous in-depth study) has been a general dumbing down to what seems an essentially simple concept, but really is something deceptively complex. The end result is that people in business, schools, hospitals and all most places of work now consider themselves 'experts' to some extent - until challenged to explain the inevitable inconsistencies or complexities in what they are saying and doing. When you start explaining some of that

complexity they will often just 'glaze over' or simply assert that they are following some recipe or formula which they have been assured is correct.

It is strange that in dealing with a concept that is so fundamental to a successful life and business, we all assume we are experts – something most of us don't feel about other vital disciplines such as medicine, engineering, religion, politics, chemistry and the law.

Fundamentally, 'risk' is about uncertainty (a much more consistently defined and understand term) and throughout history people have attempted to appreciate uncertainty so that they could better understand the future, especially when they must decide how to act.

The following is a very much summarised history of thinking about 'risk', that concentrates on the last 20 years or so and where many people now agree we've started to go badly wrong. This has led to the conclusion being shared by many across the world with much experience in the subject, that we've ended up with the 'cart before the horse': if we truly want to help people make better decisions and respond to the uncertainty present in every decision , we need to concentrate more on the process for making decisions and less on the creating the artefacts of a process that now has little real connection with normal decision-making and mostly detracts from it.

The historical background – how did we get here!

Early thinking

Over the last 10 centuries, if not longer, there are three linked, fundamental human traits that underly the development of our concept of 'risk' and how we should respond to it. Mankind:

- Likes to gamble.
- Fears the unknown.
- Always tries to understand and explain the past as a way of predicting the future.

There have been many attempts over the centuries to understand 'probability' so that we could better predict the future. I won't go through all the details of history as they are excellently summarised in Bernstein's standard reference book, 'Against the Gods'[1]

In the 20th century, milestones include:

- Work by economist Frank Knight[2], in 1921 that sought to differentiate from what he called 'risk' that was 'measurable uncertainty', and from unmeasurable uncertainty.
- John Milton Keynes[3] who pointed out that most decisions to do something positive can only be taken as a result of animal spirits and not as the outcome of

[1] Bernstein, Peter: Against the Gods: The Remarkable Story of Risk, ISBN 9780471121046
[2] Knight, Frank H: Risk, Uncertainty, Profit, New York Century Press, 1921 and 1964.
[3] Keynes, John Maynard: A treatise on probability, London, Macmillan, 1921.

a weighted average of quantitative benefits multiplied by quantitative probabilities.

- John von Neuman, who invented 'Game Theory'[4], and believed that "The true source of uncertainty lies in the intentions of others" and that "Almost every decision we make is the result of a series of negotiations in which we try to reduce uncertainty by trading off what other people want in return for what we want ourselves."
- In 1979, when Kahneman and Tversky published their seminal work[5] on risk perception based on the observation that: "It's not so much that people hate uncertainty – but rather they hate losing". They explained to us that humans: "Pay excessive attention to low-probability events accompanied by high drama and overlook events that happen in routine fashion" and that: "We treat costs and uncompensated losses differently even though their impact on wealth is identical".

More recent times

Since the 1960's (and 70's, when I first started working in the area) there have been three discrete streams of thinking about risk and how it should be understood. In all cases, the application was initially intended to support better decision making and not replace it or be in addition to it. The streams are:

1. **Finance and investments** – where people have both tried to understand past behaviour as a way of predicting future performance – and then try to assess uncertainty in real time as a way of maximising benefits while minimising losses during trading.
2. **Insurance** - where insurers try to form an appreciation of the 'risk' they are insuring to both set premiums and arrange their own re-insurance.
3. **Safety and reliability** – where decision makers require input to their decisions and to gain assurance that a particular situation or circumstance is "as safe as is reasonably practicable".

Originally, there was no need or motivation for the three streams to either agree on a common language to work together to form a more holistic view of risk for a whole organisation, project or endeavour. Some hardened specialists still view this as the case!

The problems with the differences in approach began to emerge in the 1980's where the European Community brought in legislation that required workplaces to 'list' 'risks' in 'risk registers'. Until that time, the safety community were very content dealing with hazards and using the term 'risk' (NB. not the plural) to denote the chance of the hazard injuring someone and the magnitude of the harm – expressed as a level[6].

[4] Von Neumann, John: Theory of Games and Economic Behaviour, Princeton University Press, 1944.
[5] Kahneman, Daniel and Tversky, Amos: Prospect theory: an analysis of decision under risk, Econmetrica, Vo 47. No. 2, pp 263-291, 1979.
[6] See, for example: IchemE, 1985, Nomenclature for Hazard and Risk Assessment in the Process Industries, ISBN 0 85295 184 1.

This thinking was extended in the late 80's and early 90's to environmental hazards but the approach soon became mired in the tricky problems of defining what 'harm' is, what the target was, and how that might be harmed in the short, medium and long term – and how all this might be combined to produce a level of risk.

Until the mid-90's 'risk assessment', as it had become known, was always applied on a sector or aspect basis. That is, an organisation might undertake separate risk assessments pertaining to safety and environment, etc. and the term 'risk management' was used, almost exclusively, for insurance practices.

At this time were also early approaches to apply risk assessment and reliability approaches to organisational change, contract validation, procedure development etc[7]. But no one attempted to apply these more holistically.

In the financial sector, tools were developed that attempted to understand the variations in markets so that traders could buy and sell assets (or their derivatives) in the most effective way and to know when to stop a particular transaction (stop loss limits).

The first approach I'm aware of that attempted to produce a more holistic approach to the assessment of risk was the Norwegian: *Standard NS5814:1991 "Krav til risikoanalyse*. This principally described an approach for what the Norwegian's called a 'Total analysis of risk". In the late 1980's I was working for the Norwegian consultancy, DNV Technica, and at the time helping a Norwegian petroleum company analyse the risk to safety (employees and the public), environment and project quality for a sub-sea pipeline using one approach[8]. Most of that thinking found its way into the Norwegian standard.

In the 1990's there were some early attempts to extend this approach to business as a whole and the concepts of Enterprise Risk Management (ERM) and Enterprise-wide Risk Management (EWRM) were promoted, particularly by the 'Big 5' Accounting Firms. However, in general this was largely at a conceptual level.

I built on that in 2002 when I became global manager, Risk Management for BHP Billiton and we rolled out the first EWRM approach to a large, global resource company[9]. This focussed on encouraging decision makers to properly consider the sources of uncertainty in their assumptions when faced with a decision. My remit was primarily to infuse the sensible 'risk-taking' culture of the South African based Billiton, which had led to spectacular growth, with the stodgier, 'we know better' attitude in BHP, that had almost brought it to its knees.

---

[7] See as an example of Organisational HAZOP in Purdy G: Holistic Risk Management in a Changing Energy Sector, Proceedings Of Energy Risk Management and Insurance Strategies, IIR Pty Ltd, 23rd - 24th June 1997, Melbourne

[8] Purdy G: A Practical Application of Quantified Risk Analysis, from Human Factors and Decision Making: Their Influence on Safety and Reliability, Elsevier Applied Science, pp139-157, 1989

[9] Purdy, G: Risk, Governance and Mining, Keynote Address to be given to the Mining Council of Australia at the 2003 Minerals Industry Seminar, Canberra, Tuesday June 3rd 2003.

AS/NZS 4360 – 1995, 1999 and 2004[10]

In 1992, under the auspices of Standards Australia and Standards New Zealand, a committee was formed which attempted to align the different streams of thinking about risk assessment under the umbrella of 'risk management'. The committee had representatives from many disciplines and attempted to align all approaches and languages to define a holistic approach to not just assessing (including analysing) risk but also making decisions on how risk should be responded to, or 'treated', as the standard explained.

In the 1995 and subsequent standards, Risk was defined as "the chance of something happening that will impact objectives", which attempted to align those who thought risk was an 'event', with those where the selected event was irrelevant and it was only the impact that mattered and, also, with those who worried about the context and how decisions could be made about acceptability of levels of risk and the need for treatment or not.

It also sought to satisfy those who did not necessarily regard risk as negative, but rather as uncertainty that, if responded too appropriately could lead to gains rather than just losses.

Importantly, the definition recognised that the context for risk was always the organisation's highest-level objectives.

The committee expressly did not define what a 'risk' is, as the standard was concerned with the management of risk and not of 'risks'.

Important elements of AS/NZS 4360 are that:

- Before any identification or analysis, the assessment process should commence by the context being established through the consideration of relevant factors in the internal and external environments – very much as the strategic planning process does now. This 'establishing the context' led to the identification of 'risk sources'.
- Involvement of stakeholders through communication and consultation from the beginning and throughout the process was vital.
- Organisations should adopt a system (called later a 'framework') with the express purpose to integrate or 'embed' the risk management process into their normal management and decision-making processes.

The 1999 and 2004 versions of the standard just refined the thinking in the original standard. I joined the committee in 1999 and continued to chair it for 10 years co-authoring the 2004 standard and many other published guidelines under AS/NZS 4360.

[10] Risk Management: AS/NZS 4360:2004, Standards Australia and Standards New Zealand, ISBN 0 7337 5904 1.

The AS/NZS standard became widely used in Australia and New Zealand and was adopted by several other countries as a national standard including China, Japan and Canada.

AS/NZS ISO 31000: 2009[11]

Pressure from Australia, New Zealand and other nations caused ISO to convene a Technical Committee to develop a global risk management standard. AS/NZS 4360 was the starting draft, and almost all the elements of that were retained in the final ISO standard.

After 5 years of global effort, the International Standards Organisation issued what has become the internationally accepted standard for the management of risk. Many countries were involved in its development but, noticeably, the USA only became involved at the very end. Many stakeholders from professional bodies were involved but notably, the safety profession declined as did the audit profession. Professional bodies for the insurance 'risk management' profession also declined involvement until the final meeting.

Important characteristics of the ISO standard are:

- A heavy emphasis on the need for a 'framework', whose sole purpose is the full integration of the management of risk into decision-making processes of the organisation
- A set of 'principles' of effective risk management that emphasise the need for integration into all decision-making and organisational processes and that risk management should always, explicitly, addresses uncertainty.
- A definition of risk as "effect of uncertainty on objectives".

The ISO standard is now the national standard for numerous countries around the world, including Australia[12] and the USA.

In Australia there have now been many guidelines published by Standards Australia and Standards New Zealand that give more details on aspects of the risk management process and in the application of the standard to particular sectors[13].

The US COSO ERM Framework

The vast Enron US energy company was always lauded as having one of the best approaches to risk management. However, when the company folded very suddenly in 2001 (due to poor risk management!), taking the audit and consultancy company Arthur Andersen with it, the 'Big Four' that remained suffered a significant dip in consultancy revenue.

It is well known that the US audit industry and associated bodies (like the IIA) then approached the US Treadway Commission to allow them to write and for it to publish a

[11] ISO 31000:2009, Risk Management—Principles and Guidelines. Geneva: International Standards Organisation, 2009.
[12] Purdy, Grant ISO 31000:2009—Setting a New Standard for Risk Management, Risk Analysis, Vol. 30, No. 6, 2010, Institute of Risk Analysis, 2010
[13] See for example, Sefton, David and Purdy, Grant: Legal Risk Management; HB296:2007, Standards Australia, ISBN 0 7337 8295 7.

guide to Enterprise Risk Management based on the expansion of the 'square' of the previous, COSO Internal Control Framework - into the 3 dimensions of a cube.

The "COSO ERM Framework" was published in September 2004 and immediately drew criticism from around the world. The document was very long, complex and was almost impossible to implement (without specialist consultant services!). It contained many contradictory statements and focussed mostly on generating lists of risks which were intended to be reported to Boards and shareholders. It has been revised since, but most of these problems persist.

The steps in the COSO process are:

1) **Discuss Risk Management Philosophy and Risk Appetite**. This introduced the woolly terms 'organization's risk philosophy and 'risk appetite'.
2) **Understand Risk Management Practices**. This suggested, controversially, that "ad hoc, informal, and implicit" approaches "left executives and boards with an incomplete view of the entity's top risk exposures."
3) **Review Portfolio Risks in Relation to Risk Appetite**. This required the reporting of an entity's "portfolio of top risk exposures affecting entity objectives" so that a Board and stakeholders can determine whether these are in line with "stakeholder's appetite for risk".
4) **Be Apprised of the Most Significant Risks and Related Responses**. This introduced the concept of "key risk indicators" and, somehow, identifying things called "emerging risks".

Despite overwhelming criticism from people working in risk management around the world, the Audit Profession worldwide has promoted the COSO document vigorously - as the only way to link risk and governance. At the time, while most of the new confections like 'risk appetite', 'key risk indicators' and 'emerging risks' were undefined or ambiguous in the COSO document, many groups then set about inventing their own definitions and rationales. That has continued to date and it's almost an annual event that some now confection is developed and promoted as essential.

In general, the COSO approach is often now described as 'list management' not 'risk management'.

The COSO approach has spawned a huge industry in risk management where the initial artefacts mentioned in the code have been expanded upon, driven largely by the audit and consulting profession and software companies around the world. One example has been the simple concept of 'risk appetite' which has ballooned into requirements for 'risk appetite statements', 'risk appetite assessments' and 'risk appetite assurance' and so on.

Risk appetite began life as a relatively simple term, largely only used in relation to financial trading and banking, in connection with what they describe as 'market risks'. Historically, traders were allowed to 'trade' within limits that stop large losses and their organisation's 'internal control' systems were designed to ensure those limits were not breached. The Barings Bank/Nick Leeson collapse in 1995 and other failures spurred

regulators in the banking and financial services sector to more tightly regulate how companies in the trading and banking sector set and enforced these limits[14].

The extension of this concept (and the consultancy income created) to a much wider range of industries, was largely promoted by the audit and consultancy companies and made its way into the COSO ERM code. While there are numerous definitions for 'risk appetite' the concept seems to have spread to many governance standards, almost without critical analysis or understanding. Some of the technical problems[15] of extending this concept to other forms of 'risk' and other types of organisation include:

- People defining risk in many different ways and measuring it in different forms;
- Not being clear if the appetite refers to individual risks or 'types' of risk or to some amalgamation or aggregation of levels of risk (and how this amalgamation can be conducted);
- Inability to give appropriate credit for existing controls, and assumptions on their effectiveness when expressing levels of risk;
- Working out how to compare, aggregate and measure risks with totally different types of consequences (e.g. if not solely $), timescales, exposure periods etc.;
- Overcoming the significant challenges to applying the concept across a portfolio, project, program or the whole organisation;
- Rationalising the 'reward' part of the so called 'risk/reward trade-off' when, despite common 'folk law', there is rarely any correlation between levels of risk and the benefits gained by exposure to it.

Similarly with the concepts and processes for generating 'risk registers', 'key risk indicators and approaches for identifying 'emerging risks', etc. All of these artefacts, that all seem to involve an adjective-noun combination, (and many more, like 'risk culture') seem to reflect risk management as being a separate activity, somewhat divorced from normal day-to-day operations of a business; where 'risks' are inherent and only need identifying or updating once a year.

All this has led to a continual flush of new inventions that are asserted as being essential. Often, prompted by the creation of new, commercial software tool. For example, this year's flavour, so far, is using IA to generate lists of risks so that managers etc. don't even have to think about them![16]

Corporate Governance Requirements

The Securities and Exchange Commission (SEC) in the USA, chiefly in response to the Enron collapse and other corporate failures promoted the COSO framework. Many of the COSO recommendations on reporting were mandated by the Sarbanes Oxley Act (SOX) 2002. This piece of legislation, and particular Section 404, has created the largest overhead compliance costs ever for US companies and 'external registrants'.

[14] See, for example, the Basle Convention on Capital Adequacy. Basel Committee on Banking Supervision, Amendment to the Capital Accord to incorporate market risks, January 1996, www.bis.org/publ/bcbs24.pdf.
[15] Purdy, G: Risk appetite, is the concept worth the risk, RiskPost, September 2011, NZ Society for Risk Management.
[16] See https://riskacademy.ai as just one example. And this is one of the better-informed ones!

While SOX 404 only strictly requires the listing of 'internal controls' (as described in a previous COSO Internal Control framework) this has been widely blurred by many consultants to now mean 'risks' and controls.

The US SEC also requires that companies disclose their most significant 'risk issues' in their annual reports or where there is a new 'offering'. These tend to be very non-specific such as "Compliance", "Litigation", "Financing" and "Disasters". Rarely is there any estimate of the level of risk or mention of what the company does to "treat" the risk or controls.[17]

Corporate Governance has many definitions around the world and most seem to be derived from that put out by the OECD[18]. That is:

> *Corporate governance involves a set of relationships between a company's management, its board, its shareholders and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined*.

This implies that any subsidiary function, such as risk management, should only act to support the activity of making decisions - such as the setting of objectives and how these might be attained, and how performance might be monitored. It should not seek to supplant those primary functions and impose upon an organisation its own methods, artefacts or language.

However, in the 'noughties' Corporate Governance regulators from around the world, with pressure from audit bodies, started requiring the generation of various confections from COSO from companies, without really understanding what they meant or how they could be used or understood.

In 1999, the UK Institute of Chartered Accountants published its guidance to directors on 'internal controls'. This document, known as the 'Turnbull Rules', became the cornerstone of the LSE listing rules and required that a listed company board's deliberations should include:

- "the nature and extent of the risks facing the company";
- "the extent and categories of risk which it regards as acceptable for the company to bear";
- "the likelihood of the risks concerned materialising";
- "the company's ability to reduce the incidence and impact on the business of risks that do materialise"; and
- "the costs of operating particular controls relative to the benefit thereby obtained in managing the related risks".

[17] Tobin, PJ, Shiro, JJ: Corporate Risk Disclosure Consistency or Disparity, St John's University/AIG, December 2018

[18] https://www.oecd.org/en/topics/policy-areas/governance.html

It also noted that: “it is the role of management to implement board policies on risk and control. In fulfilling its responsibilities, management should identify and evaluate the risks faced by the company for consideration by the board and design, operate and monitor a suitable system of internal control which implements the policies adopted by the board.”

When the code and its application was first reviewed in 2005 there was considerable push back and criticism by many of those consulted, nearly all of which was ignored by the Turnbull Working Group in producing the next edition. Noteworthy was the surprising and strong advice of the Institute of Internal Auditors[19] in the UK that the code should be altered to state that:

- The identification of risks and responses to them should occur at the point that decisions are made.
- There are a range of responses to risk. These include but are not limited to traditional internal controls. A complete framework would recognise the validity of all types of responses, including accepting the risk.
- There are many sources of assurance that the board can receive. A key source is assurance from management, some of which comes from what we would recognise as regular reporting on strategic projects and on performance against targets. Much of the reporting that the board sees may be embedded forms of risk management, if only they were recognised as such.

This was very prescient, as emphasised by my underlining.

In Australia the first edition (2003) of the ASX Corporate Governance Principles and Recommendations contained, at Principle 7, similar requirements for risk management and ‘internal control’ (largely written by representatives of the audit profession) as in COSO and by the US SEC. This paradoxically seemed to ignore the views of the UK based professional body for auditors. That changed somewhat in later editions (now the 3rd), which references AS/NZS ISO 31000:2009 but still talks about risk appetite and risk culture (which are inconsistent with the ISO standard).

Objectives and the management of risk

The ISO Definition of ‘risk’ is now nearly 20 years old and was derived from the Australian and NZ definition stretching back to the 1995 standard. As such, objectives were taken then to mean the highest level ‘aims’ of the organisation; its mission statement, if you wish.

In the last 10 years, the term ‘purpose’ has become commonly used to be a more fundamental expression than just objectives, strategies and plans. Rather, it is the highest expression of the reason the organisation exists. Whether articulated or not, the purpose reflects both the values to which the organisation aspires and what it seeks to achieve – and is therefore the most appropriate basis against which uncertainty is evaluated in organisations.

[19] Institute of Internal Auditors, 2005: Review of the Turnbull Guidance on Internal Control – Evidence Gathering Phase. Consultation Paper, Letter to The Turnbull Review Group, Financial Reporting Council, 4 March 2005.

I am confident that if the 2009 ISO definition were updated now, the word ‘purpose’ would be substituted for ‘objectives’.

Similarly, thinking on the management of risk at an organisational level has, fortunately, largely moved on from the ‘lists of risks’ phenomena of the late 90’s and early noughties (except for those who cling to the US COSO approach). With the widespread appreciation that the management of risk will always fail to be effective if it is retained as a stand-alone activity; the management of risk is now only regarded as effective if it is ‘integrated’ fully into decision-making practices.

This is the advice given in the original 1995 Australian and New Zealand Standard and reinforced by the clear principles for effectiveness set by the ISO 31000 standard. The sole purpose of the ‘framework’ as defined in that standard is to achieve that integration.

Therefore, if we were to adopt a modern-day definition of ‘risk management’ now it would be to something along the lines of “properly considering uncertainty when making decisions”. Which is roughly where we all started out, 40+ years ago!

The fundamental problems of ‘risks’ and their lists

While an appreciation of the necessity and benefits of integration into decision making processes is widespread in the ‘risk management’ profession, as it often seems inevitable, legislators, auditors and some project management bodies still cling to the concept of ‘risks’ as being lists of things that can go wrong and ‘risk management’ as being a discrete and separate process for generating lists or ‘registers’ of these.

Mostly these lists reflect rigid and often ill-informed perceptions at some moment in time (the past) and rarely apply to any particular decision an organisation or individual is facing now or sometime in the future. As such, producing ‘risk registers’ is now generally regarded as a sterile and wasteful process that is often only undertaken to satisfy the requirement of some regulator (‘dumb compliance’). Such documents are, in reality, rarely considered when decisions are made – because they lack any relevance, and the information contained in them cannot be easily used. They really and rarely serve no useful purpose!

At best, risks (plural) might be considered to be example scenarios expressed in terms of what could happen or exist and what it could lead to described as an effect on the organisation, particular in terms of its purpose. A statement on cause or causes in each case is also often added. However, a set of these ‘risks’ will be almost certainly not be comprehensive. It cannot be!

Any ‘risk; listed in a risk register can be only regarded, at best, as just one point on a distribution of consequences and likelihoods and the approach of awarding a risk a ‘level’ taken from some form of matrix can hardly be expected to be reliable or representative of the actual level of risk. Nevertheless, this approach is widely used with no regard to context, the organisation’s objectives and the effectiveness or not of controls.

As they say: “garbage in, garbage out!”

This is why the most effective and reliable approach to treating risk is to focus on sources and common causes, not on these example scenarios and points on a distribution or, worse still simply on consequences/impacts.

Treating risks singularly like this is known colloquially as ‘whack a mole’ because you can never be confident you’ve ever treated the circumstances and outcomes that will actually arise.

There was a very good reason the Australian, New Zealand and the ISO standards defined ‘risk’ and not ‘risks!

So where are we now?

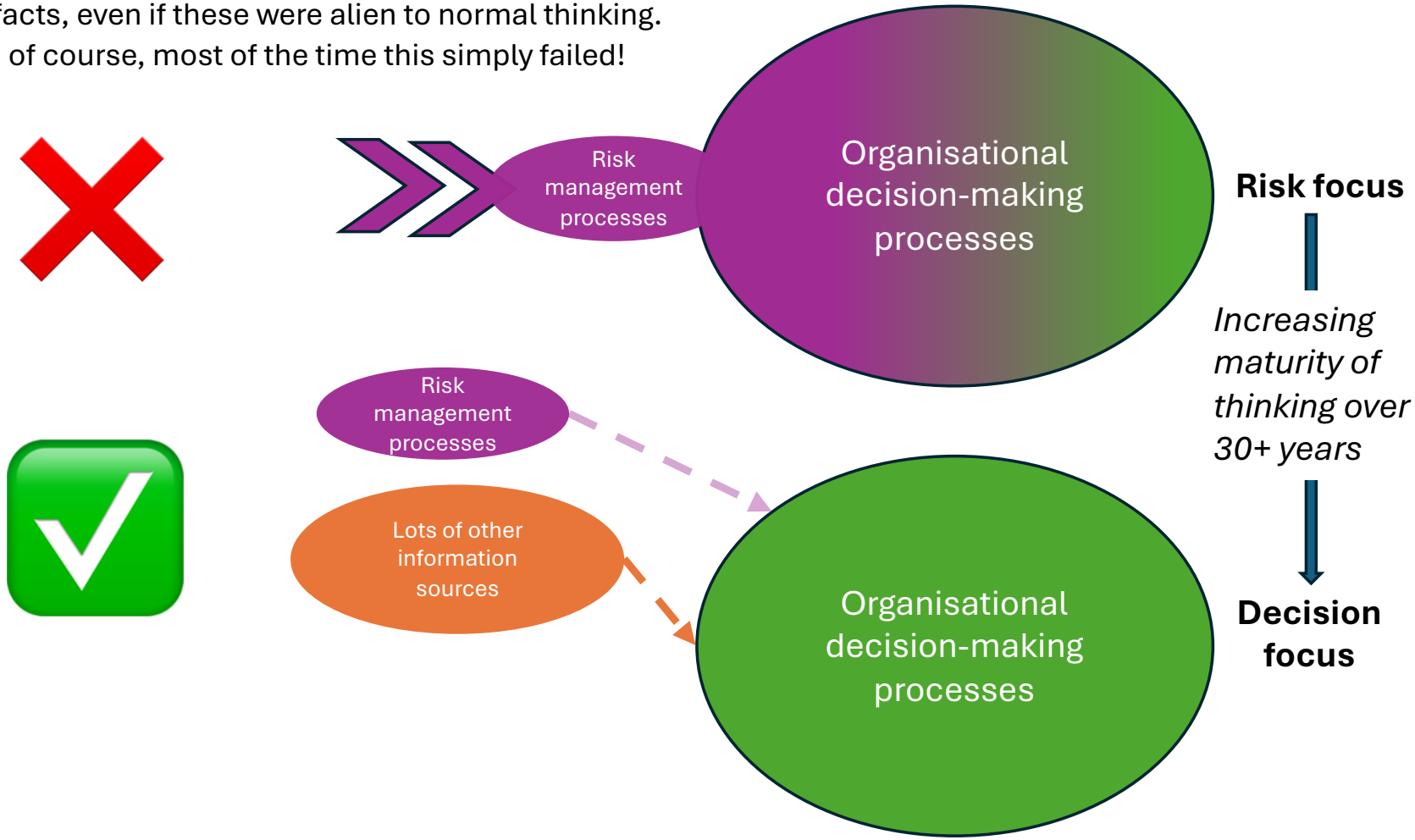
ISO 31000

After ISO 31000 was published in 2009 there was a period of reflection during which many of the original authors of the standard agreed there was an obvious dichotomy within the standard: on one hand it promoted full integration with the processes for making decision and for using a ‘framework’ to achieve that integration and, on the other, it described a discrete process for risk assessment and mentioned separate artifacts such a ‘policy’ and ‘framework’ with the word ‘risk’ placed in front of them. It became clear to all that if the management of risk had to become properly and effectively integrated in decision-making, having standalone, separately labelled artefacts and processes actually discouraged that integration.

The past and present thinking on integration is depicted in Figure 1, below. This diagram applies to both the past thinking and the COSO ERM approach vs current thinking derived from ISO 31000.

Figure 1: The concept of Integration

In the past we talked about 'embedding' risk management in decision-making. This involved decision makers adopting the RM language and artefacts, even if these were alien to normal thinking. And, of course, most of the time this simply failed!



In 2015, when it came time for ISO 31000 to be formally reviewed and possibly revised, many of the original drafters concluded that a radical revision was required, and that the obvious dichotomy mentioned above had to be resolved by recasting the standard in terms of "assisting organisations to recognize and take account of uncertainty as a part of making decisions". A design specification for the revised standard showing this recasting or re-configuration was produced, with major input from the USA (RIMS), Ireland, the UK, Demark, Turkey, Australia and New Zealand.

The new design specification was warmly welcomed by the ISO Technical Committee when first presented at its meeting in Dublin and was then sent out for wider consultation[20].

Then the pushback occurred, orchestrated by commercial interests particularly in the USA and Europe and, it subsequently transpired, stage-managed by ISO who wished to impose its 'management system standard' on all standards[21]. This management system paradigm is now causing great problems with the updating of ISO 9001, which is long overdue.

At a hastily convened meeting of the ISO Technical Committee in Rio in 2015, at which there was no representatives present that developed the design specification for the revised ISO 31000, the specification was voted down by the small number of countries present in favour of a very limited revision – which subsequently was produced.

The eventually published revision only contains some small, cosmetic changes and while it satisfies ISO's need to re-publish (and sell) standards every 5 years, most people still use the 2009 version as the standard reference.

Dissatisfaction within professional bodies

Over the last 10 years or so, there is also a parallel movement, largely driven by young people who had fallen into the risk management profession. I have witnessed they have become increasingly sceptical of their career choice because what they were required to do and the things they were required to generate are obviously regarded as largely irrelevant to the success of their organisations. They see clearly their major role being defined as one of 'compliance' and producing documents and lists of risks that no one really wanted, other than to keep regulators happy.

Many of young people (I have met) have recounted finding themselves in a 'niche', delivering a service which is not generally respected and with no obvious career progression route into mainstream senior management.

The professional organisations representing these disaffected youngsters are clearly now struggling to reconcile obvious tension between those members who are content to buy insurance and churn out annual risk registers, risk appetite statements, risk culture surveys etc. and those who consider most of this irrelevant and value destroying.

[20] ISO 31000:2009 Revision Design Specification Task Group, Project Closeout Report, August 25, 2015, document ISO/TC 262, N 201.
[21] https://www.iso.org/management-system-standards.html

Specialist risk tools and their application

These continue to be refined and developed. Reliability tools continue to be used worldwide to improve the reliability and maintainability of critical items and more generally, with other systems. As they have done, for over 60 years, they continue to provide a valuable input to decision making.

There has also been a considerable advanced in probabilistic analysis and simulation to predict the range our outcomes of budgets, project schedules and value creation. Most notably using Monte Carlo Simulation.

Particularly of late, tools have been developed to better help organisation's anticipate and be prepared for disruptions by both highlighting vulnerabilities and being prepared to take advantage of such disruptions for strategic benefit.

Nowadays, such tools are just considered one form of many sources of information that decision makers might use to inform them of uncertainties in their assumptions when making a decision.

Recognition and taking into account of uncertainty as a part of making decisions

Although the design specification for the revision of ISO 31000 was curtailed, the central principle that risk management should become an integral part of day-to-day decision making, was and continues to be widely accepted.

Most risk management professionals and their associations (such as RMIA, Risk NZ, RIMS and FERMA) around the world are starting to recognise the folly and pointlessness of compliance-driven activities that generate lists of risks and other artefacts that are described as 'risk-something or other'. Of course, many un-informed regulators still require the productions of such documents and particularly in the USA they are still seen as necessary for governance oversight purposes. Thankfully, with some exceptions this is increasingly not the case in Australia.

Because of all this, reverting to the original motivation of risk assessment, as just one means to provide information on the uncertainties that underly all decisions, the language and approach of the profession is being significantly re-framed to align with decision-making. What used to be called 'risk management practices' can now only be regarded as effective if they demonstrably creates value for decision-makers.[22]

All this comes from a long-held recognition that:

1. only by making decisions can organisations pursue and realise their purpose, and yet;
2. no decision can ever provide total certainty as to its immediate or ultimate effect.

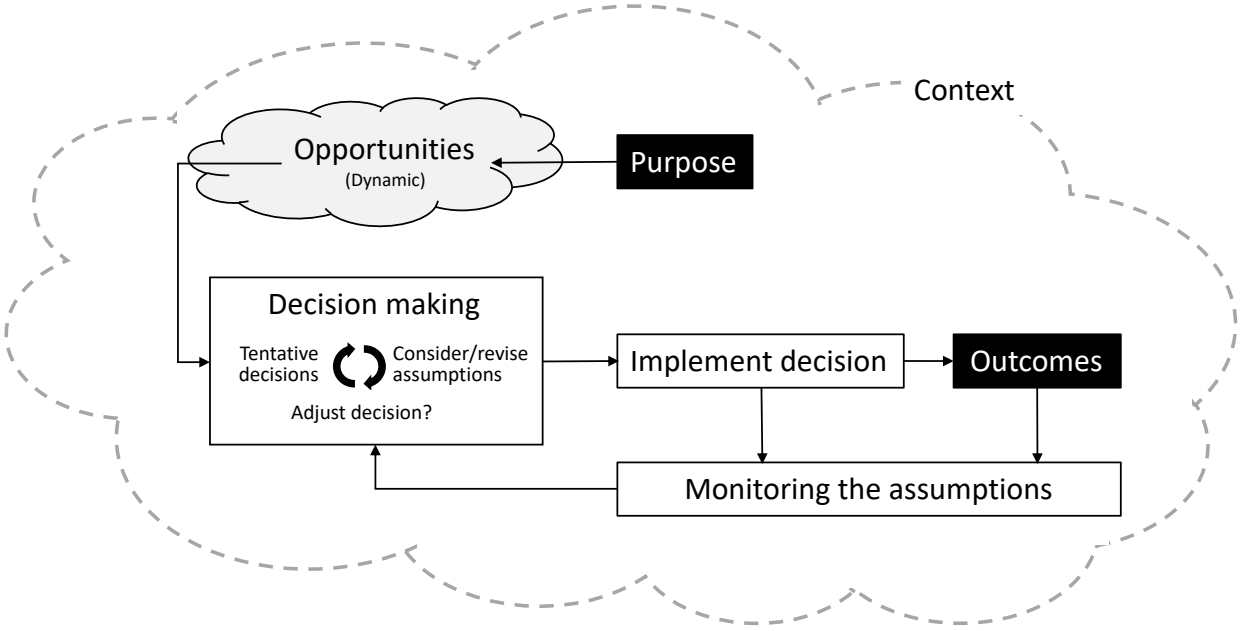
Internationally, attention is now re-focussed on optimising the steps of the process that organisations and individuals all take in making decisions. That is:

[22] See, for example the proceeding of Risk Awareness Week, 2024. https://2024.riskawarenessweek.com

1. Being clear about the organisation's Purpose.
2. Being explicit about the opportunity in terms of its alignment with the Purpose and its achievement.
3. Being clear about the intended and desired outcome.
4. Developing tentative decisions (options).
5. Considering context (internal, external and wider) and recognising assumptions and their significance.
6. Adjusting the tentative decisions (comparing options) and adopting secondary elements that will reduce uncertainty in outcomes.
7. Finalising and implementing the decision (including communications),
8. Installing form of monitoring, to detect variances in assumptions, including in actual outcomes, and then responding to amend the decision or it secondary elements

The model below is used to summarise that thinking.[23]

Figure 2: Universal Model for Decision Making



[23] Taken from Estall R and Purdy G: Deciding, a guide to even better decision making, ISBN 979-8632417471

Summary – the current two approaches to risk management

While the 'decision-making' approach described above has growing acceptance by the risk management community and is largely consistent with the criteria for effective risk management set in ISO 31000, the older COSO-derived approach with a 'risk reporting' focus is still being advocated by some regulators, particularly in the USA and in associated codes.

There also persists a third, insurance based stream where 'risk' refers to the property or organisation being insured.

Figure 3, below, shows how those three approaches have changed over time, particularly how the risk reporting focus has become more complex, while the decision-making focus has become simpler. I've also depicted how the ASX requirements have changed over time.

Grant Purdy **August 2021**

Figure 3: Current, alternate approaches to risk management