ISO 31000:2018

The Case for Reform



Dr Carl A. Gibson
Jason Brown
Dr Elizabeth M. Gibson

ISO 31000:2018

The Case for Reform

Dr Carl A. Gibson, Jason Brown and Elizabeth M. Gibson

All illustrations are the property of Executive Impact Consulting Pty Ltd, unless otherwise noted.

Copyright ©2023 Executive Impact Publishing

The moral rights of the authors have been asserted

For information about permission to reproduce selections in this book contact the info@executiveimpact.com.au

Composition and book design by Executive Impact Publishing an imprint of Executive Impact Consulting Pty Ltd.

All rights reserved. Except as permitted under the Australian Copyright Act 1968 (for example fair dealing for the purpose of study, research, criticism of review). No part of this Whitepaper may be reproduced, stored in a retrieval system, communicated or transmitted in any form or by any means without prior written permission. All inquiries should be made to the publisher at the email address above.

The material contains research studies, critical review of the ISO 31000:2018 Standard, and anecdotal commentary. This by necessity means that some assertions in this Whitepaper may prove to be incorrect as and when further information is made available in the public domain. The authors apologise in advance for any situations where this may occur in the future.

Limit of liability/ Disclaimer of warranty
While the publisher and authors have used their best efforts in preparing this Whitepaper, they make no representations or warranties with respect to the accuracy or completeness of the contents of this Whitepaper and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales material. The advice contained herein may not be suitable for your situation. You shall be liable for any loss of profit or any other commercial damages, including but not limited to direct, special, incidental, consequential, or other damages.

The authors

Dr Carl A. Gibson

Carl has held senior executive positions in government and the private section within Australia, and has advised government and private sector organisations in Canada, China, Indonesia, PNG UK, USA, Singapore, South Africa, Thailand, and the UN. He is currently a director of Executive Impact Consulting. Carl has been involved in developing standards since the mid 1990's and has contributed to the development of national and international standards, including publications in risk, resilience, governance, business continuity, crisis management, security, and fraud and corruption control. He is the lead or co-author of over 140 publications, including books and journals in a diverse range of subjects including, uncertainty and risk, critical incident management, disaster health, emergency management, infectious diseases, pandemic management, neuropsychology, and adult learning. He is a Fellow of the Australian Risk Policy Institute, The Institute for Strategic Risk Management, and the Institute of Economic Research – Australia.

Correspondence about his Whitepaper should be sent to cgibson@skymesh.com.au

Jason Lugh Brown

Jason is currently the Principal Advisor on Risk and Security to the CEO and Board of Directors of Thales Australia and New Zealand, and is the CEO of Cinnteacht, a consortium-based consultancy in risk, security, business continuity and crisis management. He has held senior executive positions in the defence industry and in various Australian Government agencies (including as Assistant Secretary and Director General). He has served on a number of senior boards and committees in both the Public Sector and Private Institutions. He is the former Chair of ISO TC 262 (responsible for the ISO 31000 risk management Standard). Jason is a member of ISO technical committees for cybersecurity and supply chain standards. He is also the former chair of Australian Standards MB025 committee which is responsible for standards development in security, emergency management, continuity, and resilience domains. He is Chair of the Council of Security Executives and SVP for Asia Pacific for ASIS International, and is a Fellow of the Institute of Strategic Risk Management, The Security Institute, Australian Security Leaders Climate Change Group, and the Australian Risk Policy Institute.

Dr Elizabeth M. Gibson

Elizabeth has held a number of senior positions with Australian and State Governments, and in higher education. She has previously been the head of the Commonwealth's analytical laboratories in Victoria, and was Secretary of EPA Victoria. She is currently the CEO of an industry association in the resources sector. She has played major roles in raising the importance and profile of STEM subjects in secondary education, and has chaired a national committee for industry education. Elizabeth was a co-author of the Australia Standard's handbook on environmental risk, and is actively involved in improving the way that risk is addressed in public policy, and has been a member of several Ministerial advisory committees.

Contents

INTRODUCTION 1

Rationale **1**

Our approach **2**

CONCEPTUAL AND TEXTUAL ANALYSIS 3

General issues **3**
Issue: If the Standard is so good, why change anything? 3
Issue: what happened to the past, where did the present go, and what about the future? 4
Issue: generic is good, but generic is also bad 4
Issue: untested assumptions 5
Issue: ISO 31000 is the only approach 6
Issue: we are talking about ERM right? 7
Issue: are we still just listing risks? 8

ISO 31000 2018 "Introduction" section **9**
Issue: a too narrow focus 9
Issue: conflation of managing risk and risk management 10
Issue: 1st paragraph of the "Introduction" 11
Issue: 2nd paragraph of the "Introduction" 11
Issue: 3rd paragraph of the Introduction 12
Issue: 6th paragraph of the Introduction 13
Issue: 7th paragraph of the introduction 13
Issue: Figure 1 inadequacies and flaws 14

The section on 'Scope' of the Standard **15**

The Section on Definitions (Section 4) **17**
Issue: the definition of risk 17
Issue: is ISO 31000 uncertain about the meaning of uncertainty? 22
Issue: definition of risk source 23
Issue: the definition of risk management 23

The section on principles **24**
Issue: missing the principle, a lack of attention and understanding? 25
Issue: on the nature of principles 26
The purpose of risk management 26

The section on the 'Framework' **42**
Issue: Figure 3 does not represent a 'Framework' 42

Framework text **47**
Issue: a lack of understanding about leadership? 47
Issue does the Standard know what "integration" means? 50

The section on design **52**
Issue: is there more to risk management commitment? 52
Issue: how can we know who owns risk, before we know what risk is? 53
Issue: communication and consultation the managerialism way! 54

The section on "Implementation" **56**

Issue: will implementation work in this way? 56
Issue: a superficial evaluation 56

The section on improvement 59
Issue: does the Standard understand adaptation? 59
Issue: should improvement be more than just incremental? 60

The section on "Process" 61
Issue: what is section "6.1 General" trying to say? 63

The Section on communication and consultation – section 6.2 65

The section scope, context and criteria 67
Issue: does anybody define the scope without knowing why? 67
Issue: is this all there is to context? 69
Issue: confused about criteria? 70

The section on the risk assessment process 75
Issue: is this really how we identify risk? 75
Issue: a weak analysis? 78
Issue: what about human frailty? 81
Issue: of complexity and connectivity 82
Issue: what has time got to do with it? 83
Issue: How effective are controls? 85
Issue: are we too sensitive? 89
Issue: dealing with biases and divergency 90
Issue: what happened to aggregation? 91

The section on risk evaluation 94
Issue: the Standard has no appetite for risk! 94

The section on risk treatment 98
Issue: another problem with iteration? 98
Issue: a muddled collection of options? 99
Issue: do we always need risk treatment plans? 100

The section on monitoring 102

The section on recording and reporting 103

The other bits that are missing 104
Issue: what about the decision-maker? 104
Issue: a perception of badness 105
Issue lack of consideration of risk governance 106
Issue: is there a problem with maturity? 106
Issue: confused about where the framework ends and the process begins? 107
Issue: data analytics, at least mention it 108
Issue: what has happened to the concept of a risk management program? 109

In conclusion 110

A final commentary 113

References 114

Overview and Executive Summary

ISO 31000, in its three editions, has served the global community well, becoming the world's most applied risk management guidance publication. There is much to praise the Standard for, however this does not mean that change is not warranted.

The broad risk management community does not have an agreed position on the status of the 2018 version of the Standard, and whilst there are numerous different views about its standing, they can be characterised as, ISO 31000:2018 is:

- Perfectly acceptable and requires no change.
- OK, but COSO is better.
- Not great, but it's better than the alternatives.
- Satisfactory, but there are some small improvements that can be made.
- Too complex, and something even simpler is needed.
- Academically unsound and should be totally abandoned in favour of science and statistics-based models.
- The wrong type of Standard, principle based does not allow compliance to be certified, and it all needs to be changed to a management system Standard.
- Is based upon a reasonable approach, that needs a substantial reform based upon evidence not conjecture.

From each proponent's perspective, their viewpoint is reasonable, and reflects how valuable they believe ISO 31000:2018 to be, and how useful it will be in the future.

This Whitepaper has its genesis in our observations of an unstructured debate that has been swirling around in governments, industry, not-for-profits, academia, professional bodies, in the 'hallowed chambers' of various national standards bodies and within ISO TC 262 (the technical committee responsible for the risk management Standard), and the across many other ISO technical committees.

The authors of this Whitepaper hold strongly to the last of the above dot points. We believe that, notwithstanding the success to date of ISO 31000, that there is much about the Standard that needs to change, because the current version of the Standard:

- Is not based upon robust peer reviewed evidence, and in parts it conflicts with or ignores the relevant discipline knowledge (in fields such as uncertainty, probability, decision-making, psychology, and management theory).
- Is largely based upon conjecture and personal beliefs of those involved in developing the Standard.
- Does not live up to its bold claims to be suitable for all types of organisation and for all types of risk.
- Is highly generic, which has led to its application in contexts for which it is not suitable or relevant.
- Does little to prevent (some would argue it encourages) the spread of poor practices and mathematical misunderstanding, which in turn results in analytical products that can be ill-informed and inaccurate.
- Has resulted in a 'risk industry' that predominantly produces 'lists of risks' of questionable value, whilst doing little to actually reduce uncertainty in decision-making.

Accordingly, we have developed a case for the reform of ISO 31000:2018, not to abandon the current Standard, but to build upon that which is 'good' and to change that which needs to change. In this respect we seek to provide input into the official deliberations of ISO about the future of the Standard that have commenced in late 2023 and will continue through 2024.

Our case for reform highlights the following, areas for change:

- The Standard is highly generic. This has been a strength of the earlier versions of the Standard, allowing its ready adoption by a wide range of users, including those with a low knowledge and experience base about risk management. In this latest version of the Standard, this generic guidance has become a weakness. The Standard has helped to promote a whole range of questionable practices, to the extent that the effectiveness and value of risk management is uncertain in many organisations.
- Unproven claims made within Standard, particularly about its wide applicability and benefits, have result in the adoption of the Standard for purposes for which it is wholly unsuitable.
- The Standard is 'confused' about its scope. For example, does it aim to provide guidance to help manage organisational/enterprise risk, or does it seek to have a much broader influence?
- A great deal of the Standard is conjecture, based upon assumptions that have not been surfaced, tested, or validated.
- The Standard ignores a great deal of the high quality published literature that deals with uncertainty and risk. In doing so, the Standard uses concepts that are outdated and in various parts of the publication are incorrect.
- The Standard presents itself as the de facto approach for managing risk, without proof. It is also a claim rejected by numerous domains that use risk assessment and have formal approaches for managing risk.
- The Standard seems to be confused about the difference between 'risk management' and 'managing risk'.
- Under the 'reign' of ISO 31000, the outputs of risk management activities have become more and more about populating 'risk registers' and creating lists of risks.
- The idea behind introducing explicit "principles" into the Standard was a meaningful innovation. However, the execution of the idea has resulted in a poorly written set of short generic statements that appear to be given 'lip-service' or totally ignored by many practitioners. A revision of the Standard needs to determine if these are the most relevant and important principles, and how they could be better explained.
- The risk management framework guidance in the Standard is incomplete and confused, and requires a major revision if it is to effectively provide usable practical guidance.
- The Standard promotes the use of a PDCA (plan-do-check-act) cycle, that has provided sterling service for almost the last 100 years, as an improvement process. The world has changed considerably in that time, and far more agile and flexible processes have since been developed to address the high complexity and uncertainty within which most organisations now operate.
- All of the processes described in the Standard are highly linear in nature, which can increasingly struggle as complexity and uncertainty increase. There are a wide range of different process models that are used in modern organisations, and the Standard needs to show how these can be applied to enhancing risk management.
- This linearity problem also extends to the 'new' version of the risk management process shown in the Standard. In particular, the redrawing of the risk management process has been a retrograde step form previous versions and has lost key aspects of meaning that was designed into the original risk management process on which ISO 31000 was based.

- There are numerous technical errors throughout the text of the Standard as well as misleading diagrams that need to be corrected. For example, describing an improvement process diagram as a 'risk management framework'.
- The definition of risk provides the foundation for how risk is conceptualised, how it is assessed, and ultimately how it is dealt with. The current definition of risk has been criticised from many different experts and commentators, and needs to be reconsidered in light of our changing understanding about the nature of uncertainty and risk.
- The concept of uncertainty is central to both the Standard's definition of risk, and to our understanding of risk. For a concept so important to and a foundation of ISO 31000, the actual concept of uncertainty is almost completely ignored in the body of the Standard.
- The Standard places a great deal of emphasis on the 'integration' of risk management, without really explaining what integration looks like, what it comprises, or how it could be achieved. This Whitepaper also posits that 'integration' may not be what is actually required.
- Much of the Standard's content about various activities that comprise risk management is superficial and incomplete. In its current form it provides little practical guidance, and this has led to the adoption of a whole range of dubious practices by practitioners.
- Many mature risk management approaches are centered on the relationships between uncertainty, risk, and decision-making, and view the core of risk management as reducing the uncertainty in a making a decision. These are concepts that are almost completely absent from the Standard.

Overall, the current version of ISO 31000 appears to be based on the process and organisational models that predominated in the 1980's. A revision of the Standard needs to ensure that its underlying thinking better reflects the contexts face by contemporary society.

Dr Carl A. Gibson
Jason Brown
Dr Elizabeth M. Gibson

Australia, November 2023

ISO 31000:2018 The Case for Reform

"*The most difficult subjects can be explained to the most slow-witted man if he has not formed any idea of them already; but the simplest thing cannot be made clear to the most intelligent man if he is firmly persuaded that he knows already, without a shadow of doubt, what is laid before him*." Leo Tolstoy.

Introduction

Rationale

ISO 31000:2018 Risk management-Guidelines[1] is soon to come to the end of its 'life' as a current International Standard, and the formal process will start, under the auspices of the International Standards Organisation (ISO) Technical Committee for risk management (TC262), to review and revise the document. Given the nominal timeframe for standard's development, a most probable publication date will be in late 2024 or early 2025. Although 'ISO 31000' has been a phenomenal success in its acceptance and take-up worldwide, the Standard is not without serious conceptual problems and practical limitations. The Standard has been widely criticised by various practitioners, professional bodies, academia, and by risk experts in different industry, science and technology domains. It is therefore timely, before ISO TC 262 deliberations get up a full head of steam, to provide a discussion Whitepaper to help inform national and international deliberations.

It can be argued that the simplicity and accessibility that has made ISO 31000:2018 *the* global guidance document, may also be responsible for both preventing the adoption of better practices (scientifically validated), and for promoting an increasing misunderstanding about the nature of risk and its management. Indeed, it appears that many of the problems in contemporary risk management arise from a shallow understanding of the Standard and the nature of risk, as well as from problems innate to ISO 31000 itself.

A Whitepaper of this nature can be seen by many as negative criticism of a widely popular Standard. However, we wish to point out that despite its problems, ISO 31000:2018 still has some well thought-out and useful content. Our intent is to help drive an improved international risk management Standard that is more practically relevant and more scientifically defensible.

[1] Australia has adopted the Standard as AS ISO 31000 2018. Note that the 2009 version and its precursor '4360' were joint Australian and New Zealand Standards. Under its current 'user pays' model, New Zealand Standards decided not to adopt the revised 2018 version of the Standard.

In doing so we will start off by asking two simple questions:

- How do we all know that ISO 31000:2018 actually works as intended?
- How do you, the reader, know that your application of ISO 31000:2018 works effectively and consistently in your own organisation?

If you suffer from any hesitation in answering *both* of these questions, then there is a serious problem that needs to be resolved.

ISO 31000 has some good foundations, that should be strengthened and built upon. However, there are examples of poor quality advice within the document that need to be rectified in its next version. Up to now, the development of ISO 31000 has been undertaken with little, if any, reference to or application of the scientific research into uncertainty, decision-making, or risk. To a large extent, the Standard remains the product of belief and conjecture, and in its vagueness, ambiguities, and silence promotes practices that are also largely devoid of supporting scientific evidence.

Our approach

This Whitepaper is based upon an analysis of the ISO 31000:2018 Standard, and considers the concepts and contentions presented in the Standard for:

- Ease and consistency of understanding.
- Relevance and applicability.
- Accuracy, validity, and evidential support.
- Prospect of achieving the intended outcomes.

The analysis and review are conducted and reported as a critique of the Standard as a whole, and a more detailed critique of each individual section of the Standard. Where appropriate we provide uplift recommendations for consideration by the reader and as input into discussions about the future of the Standard.

There are also a number of issues discussed in the Whitepaper that are not about problems within the current version of ISO 31000, but are concerned with proposals to introduce contentious concepts into the Standard in its next revision, such as changing it from a principles-based Standard to a Management System Standard (MSS)[2].

[2] Whether it be for full mandatory compliance requirements as in ISO 9001 (a type A MSS), or more discretionary in nature (type B MSS, such as ISO 9004), where Type B MSS are often developed to provide guidance to implement a type A MSS.

Conceptual and textual analysis

General issues

Issue: If the Standard is so good, why change anything?

There appears to be a wide acknowledgement of ISO 31000's position as one of the best 'methodological' guidance documents on risk management, and the almost ubiquitous global adoption (certainly outside of the USA) seems to support this contention. Indeed, ISO 31000 does not appear to suffer from many of the problems innate to the USA's COSO Standard (COSO, 2017). Conversely, the COSO Standard is less vague, provides greater detailed guidance, and more informative diagrams, despite its other flaws. All of which are key issues for the current ISO 31000:2018.

Support for the effectiveness of ISO 31000, up to now, has been largely based on anecdotal experience and unevidenced claims (see below). Whilst a range of studies published in reputable peer-reviewed journals have been critical of the use of such a Standard (Aven and Ylönem, 2019; Wiegman et al, 2017; Brunsson et al, 2012; Rowley 2007; Hallström et al; Timmermans and Epstein, 2010; Hallström 2004)[3].

There are a few studies that show *correlation* between the presence of risk management within an organisation and improved performance, but these do not include any rigorous study on the actual efficacy of the application of the ISO 31000:2018 framework or process. There is evidence of a high *correlation* between organisations that have in place formal structured approaches for managing risk, but the evidence for any causal relationship between the use of ISO 31000 and improved organisational performance is very weak (discussed in detail later in this Whitepaper). Where such positive correlation exists, this could simply be explained by the situation of organisations that use risk management Standards also having management and staff that are more aware of risk, and more willing to make informed decisions about risk. Improved organisational performance is also probably more to do with an elevated focus on improving controls in these organisations, then anything to do with the actual measurement and reporting of risk contributing directly to improved decision-making.

It has also been argued that the very conceptualisation of risk within ISO 31000:2018 is not meaningful and "could seriously misguide decision-makers" (Aven and Ylönem, 2019). The very fact that such a claim has been made should result in ISO TC262[4] undertaking a serious consideration of its conceptualisation of risk.

Overall, the Standard suffers from one major flaw, it conceptualises the real world in overly simplistic terms, and tries to explain risk management in similar terms, often using a range of concepts that do not align with either the science or with better practices. This may be partly due to the desire to make ISO 31000 a concise document, however when brevity removes meaning and hinders understanding that is not a good Standard.

[3] Although some of these criticism predate the publication of ISO 31000:2018, they are still valid today for the current version.

[4] The ISO technical committee responsible for ISO 31000 and related Standards.

Resolution
Despite the existing value that the Standard provides, it is apparent from the research and better practices discussed in the findings of this Whitepaper that a simple revision of ISO 31000 would be inadequate, and that there is a compelling argument for the complete reform of the Standard.

Issue: what happened to the past, where did the present go, and what about the future?

Perhaps one of the most outstanding things about ISO 31000:2018 is that in providing guidance on risk it completely fails to mention 'the past', 'the present' and the 'future'. This is amazing, considering that risk is all about uncertainty about future states (Blockley, 2009), and is informed by past experience, and by situational awareness about the present. How anyone can gain an understanding of risk (and by extension, risk management) without even considering these three temporal concepts is a serious omission.

Resolution
Any conceptualisation and consideration of risk needs to include some discourse on the relevance of past, present, and future states.

Issue: generic is good, but generic is also bad

One of the admirable features of ISO 31000 is that it aims to be non-prescriptive and to provide a Standard that is generic enough so that it can be customised to fit different contexts and different organisational needs[5]. It has also been argued that because the Standard is so generic (and broadly principles based), that it naturally aligns with the overall form of many other traditional management processes present in organisations (Lalonde and Boiral, 2012).

In fact, the Standard is so generic that in many parts of the document the word 'risk' could be deleted (and then left alone or another word such as 'governance' or 'quality' be substituted) and the Standard would still make equivalent sense for other management activities. That is understandable, since many of the components of the Standard have not come from the scientific literature on risk, but instead have been copied over directly from other traditional management practices. Differing only in detail and evidence of efficacy.

One of the commonest criticisms of the Standard is that because of this generic nature, it provides little actual practical guidance. Since much of the text is generic, vague, ambiguous, or lacks coherence, the interpretation of meaning relies heavily upon each individual reader's knowledge and experience, resulting in a wide range of inconsistent and incorrect beliefs about the guidance. This means that to interpret and apply the Standard is highly dependent upon a user's individual assumptions, which are rarely acknowledged, let alone tested. This also results in the belief that the

[5] This is an important consideration, since such flexibility is often lost in the adoption of Management System Standards.

Standard states things that it clearly does not[6], furthering the continuance of poor practices, inconsistencies in application, and even fundamental misunderstandings about uncertainty and risk.

Issue: untested assumptions

A great deal of the content of ISO 31000:2018 is based upon unsurfaced, unrecognised, and untested assumptions of the 'writers', establishing conjecture as 'factual' guidance without supporting evidence. The development process for the Standard rarely explicitly recognises the presence of these assumptions, and even if they are surfaced, there is no system in place to rigorously assess and validate (or invalidate) such assumptions.

For example, the foundation of the Standard, the definition of risk, is laden with assumptions:

- The assumption that there is one single sentence that can define the complexity of risk, something that science-based experts have been unable to do with universal agreement over the last 100 years or more.
- The assumption that 'objectives' are the key organisational thing of value that needs to be considered.
- The assumption that 'uncertainty' is the vital element of risk.
- That 'uncertainty' can exert an 'effect' (especially since 'uncertainty' does not appear to be well understood within the Standard).
- The assumption that uncertainty can affect objectives.

This is not saying that all or any of these assumptions are not valid, they very well may be. However, until they have been validated and the Standard can justify their presence, then they simply remain as unproven conjecture.

Resolution

In the forthcoming revision of ISO 31000 all key concepts and assertions (and their underlying assumptions) have to be rigorously challenged, and evidence provided in support. There are broadly two ways to help deal with the issue of assumptions. Building and reconfirming concepts for inclusion in a revised Standard requires a foundation in good research. We recommend that for each of the key concepts which form the basis of and guidance for ISO 31000, that a whitepaper is developed looking at the historical evolution of the concept and the peer reviewed published evidence in support of the concept[7]. This suite of whitepapers would then form the reference documents for writing relevant sections of the Standard, and can be expanded later into more specific and detailed guidance handbooks.

There are a wide range of techniques available for surfacing and testing assumptions (UFMCS, 2016), and suitable techniques should be employed during the development of the various drafts during the Standard's revision.

[6] There is considerable anecdotal evidence gleaned from training courses, workshops, conference, publications, personal communications, and reviews of organisational risk management arrangements that demonstrate the extent of these misunderstandings.

[7] And where applicable the rejection or modification of the concept.

Where robust evidence is lacking, content that is shown to be conjecture has to be either removed from the document or identified as such. Within some Australian Standards working groups, for both writing and reviewing draft documents, we have adopted a simple information rating system, which could serve as a model for ISO Technical Committee 262:

i. Is the concept supported by published robust (preferably peer-reviewed) evidence?
ii. Is the concept experientially supported, i.e., is it based upon widespread generally accepted practices (which are not controversial), or widespread multiple and consistent experiences?
iii. Is the concept conjectural, i.e., unsupported by robust defensible evidence?

For concepts determined at (ii) or (iii), it is then incumbent upon the proponent of the concept to provide further evidence at an elevated level for it to be accepted.

Ultimately, the decision on whether to include a concepts depends upon this assessment of the overall weight of supporting evidence.

Issue: ISO 31000 is the only approach

Overall, ISO 31000 tries to establish that it is the only meaningful approach for managing risk. Although much of this is by inference and allusion, the Standard does also make this explicit in statements in several places within the Standard, such as "*Managing risk* is based upon the principles, framework and process *outlined in this document*, as illustrated in Figure 1", (our emphasis in italics).

This is clearly a misleading statement. There are multiple different ways of managing risk which have no resemblance to what the Standard calls a 'risk management framework', or 'risk management process'. ISO 31000 cannot even claim to be ***the*** risk management approach, it is only one of many different risk management methodologies (for example: US EPA, 2023; Boon, 2022; Meyer and Reniers, 2022; Roseke, 2022; Safe Work Australia, 2022; Hubbard, 2020; Kernchen, 2020; EPA, 2021; American Diabetes Association, 2019; Aven, 2019; Fan and Stevenson, 2018; Prince2, 2018; Muralikrishna and Manickam, 2017; Boyce, 2013). Furthermore, there are also many organisations that use 'organisational risk' or 'enterprise risk' approaches that find that the COSO risk management approach is better suited to their needs. Even within the International Standards Organisation itself, the 'superior' position of ISO 31000:2018 is widely and strongly contested, to the extent that not only the risk management framework and process, but even the risk definition is rejected by a significant number of ISO Standards that reference risk (see below). Once we leave behind the domains of 'organisational risk' and 'enterprise risk', the acceptance and use of ISO 31000) is rarer still.

Resolution
A number of peer reviewed publications show that the Standard, although popular as general guidance for organisations, is not as widely accepted amongst, for example, science-based risk practitioners, or by financial risk specialists. Commentary within the Standard that ISO 31000 is the only, preferred, best, or most common approach for '*managing risk*' or even for '*risk management*' should be removed from the document.

Issue: we are talking about ERM right?

In recent years there has been increasing interest in the concept of 'enterprise risk management' (ERM). There have been lots of commentary and social media articles from self-appointed gurus, and online and glossy print promotions from larger consulting firms. An increasing number of organisations label their risk management approaches as 'ERM', and comparisons are made between the 'COSO-ERM approach' and that of ISO 31000. Questions have been asked frequently about why ISO 31000 does not use the term 'ERM'.

Amongst the many differences between the two risk management 'standards' documents, the major ones are around the questions of intent and focus. In addition to COSO 's audit and evaluation of controls focus, COSO is focused on 'ERM', whilst ISO 31000 is determinedly not focused on this direction, instead focusing on 'organisational risk'. If one does a search online, there is a lot of confusion and little agreement about what constitutes 'ERM'. The commonest ideas seem to be around ERM as just a 'sexier' term for organisational risk management (i.e., they mean basically the same thing), or that 'ERM' is the more encompassing way of looking at risk compared with 'traditional' risk management, where the latter has historically just looked at losses. The result has been that ERM has become, to some extent, a jargon term prominently used to rebadge risk management as a more sellable product.

If we look back on the original concepts behind 'ERM', it was to put in place mechanisms to deal specifically with risk that was of concern to senior management ('top management') and the Board, and had an enterprise-wide effect, including financial operating risk (Jankensgård, 2019; Hawkins, 2000; Slabaugh, 2000; Berry and Philips, 1998; Busman, 1998; Lewis and Mody, 1997; Levinsohn, 1998; Dickson, 1995). Enterprise risk was commonly defined along the lines of "the extent to which the outcomes from the corporate strategy may differ from those specified in its corporate objectives, or the extent to which they fail to meet those objectives" (Dickinson, 2001). Those risks that were more operational, tactical or 'specialist' (such as project risk, health and safety-related risk, security-related risk, manufacturing process risks, marketing-related risks, etc.) were excluded from the conceptualisation of 'ERM'. Over the intervening years, almost everyone that has used the term 'ERM' has put their own interests and perspectives into its meaning, so that today we have such a hotchpotch of ideas, that the term is probably undefinable.

ISO 31000's outlook, however, was across all types of organisational risk, whether strategic, operational, or tactical, and irrespective of whether risks were relevant across the whole of an organisation, or involved risk specific to individual activities. Retaining its more encompassing general perspective, and avoiding getting drawn into the 'ERM fad' is one of the great strengths of ISO 31000:2018.

Resolution

ISO 31000's wide perspective on risk is a strength and needs to be maintained, the revision of the Standard also needs to recognise that 'ERM' is a confection, and means so many things to many different people, the term on its own is effectively meaningless. When organisations practice risk management, their focus may be across the whole of an organisation, or it may be upon specific contexts and activities. It does not matter, it is all still ***risk management***.

Issue: are we still just listing risks?

A common criticism of ISO 31000 since it was first introduced in 2009, was that it created a practice of "listing risks" (Leitch, 2016; 2012). Whilst this criticism may have been valid for the 2009 version of the Standard, is it still true for the 2018 version?

Certainly, this most recent version of the Standard neither mentions "risk lists" nor "risk registers" (the common option for recording these 'lists'). However, it could also be argued that the content of the Standard, and it's almost complete silence on the different types of risk information (and how the information can be used), has encouraged the continuance of 'risk listing'. Anecdotally, this still seems to hold true, as it appears that for many 'risk practitioners' the majority of their efforts and time is spent on creating these 'lists of risks', recording them into 'risk registers', and extracting summary sub-lists for reporting purposes[8].

Resolution

The Standard currently alludes to, but is not explicit enough that the purpose of risk assessment, and by extension - broader risk management, is to build a body knowledge about a 'problem' and ways of solving this 'problem' to enable informed decisions to be made about uncertainty and risk (Aven, 2016a). The Standard's guidance on the outputs of the risk management process and their uses needs to be strengthened considerably, to include those situations where quantitative metrics versus narrative constructs can be most meaningfully applied.

[8] We are aware of multiple instances where senior members of different organisations' Boards have requested of their respective 'risk managers' that the entire list of risks in the register be extracted into a paper report. By way of example, in one particular case, this Board report was a list of qualitatively rated risks, one risk per line in the report table, comprising 88 pages in total. One of this particular risk manager's personal performance criteria was to produce this list of risks every two months for the Board. The main outcome of this reporting was to provide some of those on the Board with a nice warm feeling that someone, somewhere, and somehow was "looking after risk", which seemed to be the full extent to which the lists of risks was used.

ISO 31000 2018 "Introduction" section

The Introduction to ISO 31000:2018 provides a series of statements about managing risk, that seek to justify the approach taken by the Standard. Although essentially high level and generic statements, there is nothing majorly 'wrong' with these individual statements, and they do provide some positioning for the justification for *managing risk*[9].

Issue: a too narrow focus

The "Introduction" section firmly establishes a limited focus for the Standard, namely on organisational risk (which is commonly misinterpreted as the even narrower concept of 'enterprise risk'). This (intentionally or unintentionally), has the very real potential to limit the thinking that underpins the Standard, the way in which the Standard is interpreted, and the manner in which it is applied.

The original Standard -AS/NZS 4360[10], on which ISO 31000 was based, tried to establish a broader remit – providing a "generic guide for managing risk". Despite ISO 31000's much narrower remit (the 'organisation'[11]), it is used frequently as the 'go to' document for a much wider application. A use to which it seems less suited, and that was more successfully achieved with AS/NZS 4360. For example, ISO 31000:2018 is used as methodological basis for a wide variety of national and societal risks, as well as for Regulations and regulatory instruments in different jurisdictions. Given that the Standard is written for use within an organizational context, the question needs to be asked about its suitability beyond this context.

ISO 31000 can work well as a risk management guide for contexts that are simple, and linear and stable, but does struggle in its use as the context becomes more complex, specialised, non-routine, or volatile. This is especially the case where systemic risk (Silmann et al, 2022; Renn, 2020; Schweizer, 2018) and 'multi-hazard' and 'multi-risk' complexes (Hochrainer-Stigler et al, 2023) are concerned. This significant limitation has been recognised both by Standards Australia's expert technical committee on risk management (OB007) and expert technical committee on security and resilience – MB025). This has resulted in significant adaptations to ISO 31000 being developed over the last decade or so and published as a separate Standard (AS/NZS 5050 - Managing disruption-related risk[12]) and a Handbook (HB167 - Managing security-related risk[13]).

The innate intention of ISO 31000:2018 appears to be for use within the organisational risk domain, outside of this domain its utility can vary context by context. The content and design of the Standard can be inadequate for considering broader societal risk, such as climatic, environmental, public safety, geological and geotechnical, financial and economic systems related risk, without substantial modification.

---

[9] But not necessarily for *risk management.*

[10] The original joint Australian and New Zealand risk management Standard first published in 1995 and subsequently revised in 1999 and 2004.

[11] ISO 31073: 2022 Risk management – Vocabulary defines 'organization' as: "person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its *objectives*", ISO 31000 repeatedly applies "organization" in the much narrower sense of common language usage as an 'enterprise' and 'entity'. This more common usage is also consistent with many other ISO Standards.

[12] Originally published as an interim Standard in 2020, and subsequently as a full Standard in 2023.

[13] Originally published in 2006, with a major revision and publication due in late 2023 or early 2024.

Resolution

We will address the issue of breadth of context and scope of ISO 31000 later in this Whitepaper.

Issue: conflation of managing risk and risk management

One of the major issues with the "Introduction" section of ISO 31000:2018 is that numerous statements conflate the concept of 'managing risk' with the concept of 'risk management' (which are very different), and in doing so try to imply that the benefits that come from *managing risk*, are automatically associated with *risk management* (which is not necessarily true). Managing risk is a much broader and encompassing suite of decisions and activities, than is considered within the narrower confines of a methodological risk management approach, such as ISO 31000.

All organisations, going back to the known earliest written records[14] (for example, *"The Instructions of Shuurupak"* from ancient Sumeria[15], circa 4,500 years ago) have purposefully managed risks by recognising hazards and threats, recognising uncertainty about the future, and doing something about it. Even today, almost all organisational structures, polices, procedures, plans, and decision-making have been put in place to provide increased certainty that objectives can be pursued successfully (i.e., manage risk). Yet formal risk management has had, and continues to have influence over only part of what constitutes an organisation.

For many organisations that use ISO 31000, their strategy and operations encompass many hundreds if not thousands of individual decisions and actions each day. Only a small fraction of which will be considered by that organisation's formal risk management approach. Simply, a majority of decisions and actions that 'manage' risk within an organisation are not carried out under the organisation's formal risk management framework, or a 31000 based (or COSO-based) risk management process. Many assessments and decisions that people make about risk are under limitations that are not conducive to using these standardised risk management approaches[16].

This is not saying that these standardised approaches should not be used, or that their use should not continue to be expanded, but rather that we all need to better understand under what situations alternative ways of managing risk should be used or not used.

Resolution

No matter the success of any risk management endeavour, many decisions about risk will continue to be made outside of any formal risk management framework. The Standard's "Introduction" should demonstrate the important contribution that risk management can make to managing risk, but also should make clear that formal risk management (and especially ISO 31000) is not the only way that risk is addressed. Revising the "Introduction" should also provide a focus and guidance for making decisions about where risk management should be applied, rather than just the current 'shotgun' approach.

[14] In reality, the management of risk by organised groups of people will have been practiced long *before Homo sapiens* first emerged, and will have been a capability possessed by Neanderthals, Denisovans, and probably much earlier humans where there was some ability to recognise future uncertainty.
[15] These Sumerian "Instructions" concerned the control of certain agricultural and societal risks.
[16] For example, there are many volatile or turbulent situations were a 'dynamic risk assessment' would be used in preference to ISO 31000 (see later in this Whitepaper for a discussion about dynamic risk assessment).

Issue: 1st paragraph of the "Introduction"

The first paragraph of the "Introduction" section states that the Standard is for "people who create and protect value by managing risk…". This is a rather grandiose claim for the Standard, as the statement literally includes everyone that works in the organisation. Whereas the document is, in reality, only written for the small minority that engage in the type of formal risk management activities described in the Standard. There will be many individuals with responsibility for managing different risks for which this Standard will be largely irrelevant.

Resolution
Such all-encompassing statements should be avoided in a Standard, especially when they are inaccurate and the exceptions far outweigh the inclusions. The Standard is for people that use a formal risk management approach to manage risk to achieve organisation-related objectives.

Issue: 2nd paragraph of the "Introduction"

The second paragraph of the "Introduction" section is unnecessarily convoluted, and there are far more sources of uncertainty than are due to "external and internal factors and influences" in the common interpretation of the term. For example, consideration could also include uncertainty about data collected about a system, uncertainty about the analysts' biases and their capabilities to undertake the analysis, uncertainty within the analytical model and the criteria used, uncertainty about the applicability of the chosen analytical tools and techniques.

Even after a risk assessment is conducted, there could be further uncertainty introduced by way of decision-makers' biases or because of any limited capabilities to use the risk information and make relevant inferences, etc. There will also be uncertainty about organisational objectives (which form the cornerstone of risk management), the extent to which objectives are relevant and achievable, the extent to which the underpinning assumptions have been recognised and validated, the stability of the objectives over time, the consistency with which different individuals understand the objectives, etc.

Resolution
The entire conceptualisation of uncertainty and its association with objectives requires further research and development, including the manner in which uncertainty may influence the *pursuit and achievement* of objectives.

The revision of the Standard should also consider if 'objectives' are the appropriate 'element' in consideration of risk, or if other elements such as effect on 'outcomes', 'things of value', etc. would be more appropriate. Especially since 'objectives' are only a constructed 'target' expressing a simplified summary of what purpose, intent, and desire are trying to achieve.

Issue: 3rd paragraph of the Introduction

The third paragraph of the "Introduction" to the Standard concerns the concept of 'iteration'. There are a number of problems in the way in which ISO 31000 applies the term 'iteration'. Firstly, whilst any cyclical process could be described as 'iterative'[17], most management of risk is not iterative to any appreciable degree, i.e., the process does not *continuously* repeat itself. In situations where the process does repeat itself, it will usually be limited to only one or two additional cycles (and hence is not truly 'iterative'). In a majority of situations, 'risk' is recognised, the required actions are obvious, and they are implemented, often intuitively[18], without multiple repetitions of the 'risk cycle'. Repeating the risk management weeks, days, or months later to update a 'risk profile' or introduce additional risk treatment is not truly iterative.

The Standard fundamentally misunderstands the term 'iterative', this misunderstanding is further reinforced by its Figure 1 and Figure 4. It could be argued that the 'framework process' (Figure 3 in the Standard) has an iterative nature, i.e., the framework should continue to be revised and improved over time[19]. However, the same argument does not hold when applying the risk management process, where the aim is for the process to allow learning and modification of assessment and decision outputs to occur during the activities described by the process. Rather than continuously repeating the risk management process cycle 'iteratively', effective risk management involves revisiting activities within the process.

An iterative cycle was not the primary intent of the original risk management Standard (AS/NZS 4360) nor of the original ISO Standard that was derived from it (ISO 31000: 2009). The key process diagrams in both of these Standards clearly showed reflective, reflexive and recursive flows occurring during each of the risk management process activities. These flows are where progressive learning is used to challenge assumptions, experiences, and findings during each activity. This then allows revisiting prior activities as necessary to revise earlier findings or conduct further exploration as necessary. All of which is undertaken whilst those subsequent activities are still progressing.

The inclusion of Figure 1 and the redrawing of Figure 4 that occurred during the development of the 2108 version of the Standard has reinforced out-of-date ideas about process theory, and has almost completely removed the reflective and reflexive nature of the risk management process (and to the risk framework process as well). The highly problematic nature of these Figures is discussed in more detail later in this Whitepaper.

Indeed, it is arguable if the process is ever 'iterative'. When the risk management process is repeated, it is often a *de novo* application, repeated sometime (days, weeks, or months) after the initial use of the process, depending upon the context.

Standards Australia and New Zealand Standards jointly recognised the problems and limitations of the ISO 31000:2018 circular risk management process diagram, and the mistaken ideas about iteration. Accordingly, a new interim Standard was published in 2020 (AS/NZS 5050: Managing disruption related risk, and subsequently transitioned into a full Standard in 2023). This new Standard promoted a more organic and realistic process, which better represented how good risk management is

[17] Meaning that a step-by-step process, once it reaches the 'end' step, is then continuously repeated by using the outputs of one cycle to drive the subsequent cycle, and so on.
[18] Especially where there is a high degree of pattern recognition, and in situations where there is a need for rapid decision resolution.
[19] Meaning that as one cycle completes, it automatically generates the commencement of the next cycle. It is far more common for such cycles to be repeated periodically rather than iteratively.

practised in reality (see below). This same process thinking was subsequently adopted by Standards Australia in their recent draft revision of HB167 Managing security-related risk.

Resolution

The next revision of the Standard should determine if risk management is actually 'iterative' (according to its actual meaning) or if other concepts such as 'reflexive', 'reflective', and 'recursive' better describe the risk management process.

Issue: 6th paragraph of the Introduction

The 6th paragraph of the introduction is a statement about the need for consideration the internal and external context. There is nothing wrong *per se* with this paragraph although it is rather simplistic and generic. However, it does ignore several key concepts about the importance of context.

Resolution: Establishing the context is not just about what is happening externally to and internally within the organisation. It is also, more importantly, about the manner in which the external context interacts with and influences the internal context. This concept should be explained in the next revision of ISO 31000.

Issue: 7th paragraph of the introduction

Perhaps the most significant conflation of concepts within the Standard is in this paragraph of the "Introduction" section. The final paragraph of the section categorically states that "*managing risk* is based on the principles, framework and process outlined in the document" (our emphasis). This is manifestly incorrect. As we have already discussed above, formal risk management is only one way in which risk is managed, and ISO 31000 is only one of many different formal approaches for managing risk. Globally, the vast majority of activities directed at managing risk are not based on ISO 31000.

To illustrate this, one only has to look at all of the different ISO Technical Committees that include risk management concepts in their individual Standards, and yet strongly disagree with ISO 31000's assertion that managing risk is based upon the contents of this Standard. There are approximately 1013 different ISO Standards as well as 603 other ISO/IEC publications that include risk concepts. Out of which there are only *five* or so other Standards[20] that are fully consistent with ISO 31000 in approach taken. The technical committees responsible for these 1600 or so publications cannot even accept ISO 31000's definition of risk as being correct. In fact, they cannot even agree on a common core of a definition of risk. Even at the level of 'enterprise risk management', users of the COSO Standard would also dispute ISO 31000's assertion.

To assume that ISO 31000 is the centre of the 'risk universe' can be perceived as hubris and arrogance. This perception of centrality and the desire to promote the primacy of the ISO 31000 approach may lead to a narrow vision of the best way to address risk. As yet, there is no robust compelling evidence

[20] Outside of those produced by ISO TC262 and TC 292.

that ISO 31000 is the universally best risk management approach. As stated previously, those studies that have been conducted rely on association and correlation but *not on evidence of causation*.

Resolution

ISO 31000 needs to avoid making statements that are absolutist, conjectural, or that cannot otherwise be substantiated. This closing statement of the "Introduction" can be made more acceptable with a simple rewrite to: "Risk management, *as described in this Standard*, is based upon the principles, framework[21] and processes illustrated in Figure 1".

Issue: Figure 1 inadequacies and flaws

There are a number of issues with Figure 1, most of which will be dealt with when the individual components of the diagram are considered later in this Whitepaper. However, for now, let's consider the Framework cycle. This 'circle' diagram does not describe a risk management *framework*, instead it shows a variation of the old PDCA cycle, a planning and implementation process which could be used to implement the risk management framework (in fact any type of framework), but is certainly on its own NOT a framework. We will consider the illogical nature of the cycle in more detail later on in this Whitepaper.

Resolution

Possible resolutions for addressing the inadequacies and flaws of Figure 1 are discussed under individual issues below.

[21] Noting that Figure 1 does not actually show a risk management framework, only a process for developing and applying a framework.

The section on 'Scope' of the Standard

As we have already established, ISO 31000 does not provide guidelines on *managing risk* faced by organizations. The Standard instead provides guidelines on a *particular risk management approach*, one amongst many such approaches that exist and have been applied successfully. This Scope section also states that the guidelines can be "customized to any organization and context". Leaving out (for the moment) its application to "any organization", there is a weight of evidence and practice that shows that ISO 31000 cannot be customised to a range of contexts without significant modification, and abandoning some of its key features, such as the rigid linear risk management process (Standards Australia: 2020).

ISO 31000 provides an essentially linear risk management process based upon linear thinking[22]. The choice of language in the Standard, for example discussing risk management activities variously as "stages" or "steps", further reinforces this linear thinking. This sort of linear approach described by the Standard can work really well when the problems it is trying to address are simple or linear in nature (e.g., mechanistic). However, in socio-technical systems (which are present in most organizations) as complexity and uncertainty increase, the ISO 31000 (and COSO) model increasingly struggles. Using linear thinking and models to solve complex issues can be highly problematic (McLees, 2023; Pieries, 2022; Turner and Baker, 2019; San Cristóbal et al, 2018; Damgaard et al, 2018; Rycroft-Malone, 2018; Dörner and Funke, 2017; Knaub, 2017; Thamhain, 2019; Di Russo, 2016; Kamensky, 2011). This is one of the reasons why many disciplines have their own way of managing risk (and is a contributing reason why the ISO Taskforce on risk, with multi-disciplinary representation, has been unable to even reach a consensus on risk and risk management).

It is also the reason why Standards Australia published a new Standard (AS 5050:2020) on managing disruption-related risk, and a Handbook on security-related risk (AS HB 167) in order to address risk in highly non-routine contexts. Risk that ISO 31000:2018 on its own is not capable of addressing effectively. The international Standardization Organization also seems to recognise that ISO 31000, as a standalone standard, is not capable of dealing with certain specific contexts. Or else additional Standards for "legal risk", "travel risk", a Technical Specification on "emerging risk", and potentially over 1000 other Standards (dealing with risk differently to ISO 31000) would not need to have been developed.

This problem with ISO 31000 in its current form, by default also renders paragraph 2 of the Scope section, as untrue. ISO 31000 does not provide a common approach for managing *any type of risk* or for *any activity* (as in paragraph 3)[23]. It is also unclear how the Standard can be applied to "decision-making at all levels" as there is little robust evidence in support of this conjecture. ISO 31000's conceptualisation and focus on 'organizations' has also been subject to some criticism, as this is a far narrower application than was envisaged by the original AS/NZS 4360 Standard.

[22] Putting the process diagram inside a circle does not change its linear character.

[23] The issue of managing "any type of risk" may be better addressed directly by the inclusion of appropriate risk management guidance by the ISO technical committees responsible for specific disciplines and applications, e.g., IEC/ISO 27005 Information technology — Security techniques — Information security risk management, and others.

This has led to problems with its broader application (with little customisation) to contexts such as risk-based regulation[24], [25], health and safety-related risk, environmental-related risk, security-related risk, cyber-related risk, etc. It's use in such specific applications have remained largely unvalidated and unsupported by scientific evidence.

[24] It is worth noting that some risk based regulation has led to requirements to consider an almost infinite number of risk requiring excessive data gathering conducted over a significant number of years.

[25] For example, an attempt to apply the ISO 31000 process to risk-based regulation in Victoria, such as with the Mineral Resources (Sustainable Development) (Extractive Industries) Regulations 2015 required the use of a flawed risk management approach, resulting in both greenfield and existing quarry extension applications approvals plummet, leading to increased prices for quarry materials and heavily impacting 'big build' infrastructure projects.

The Section on Definitions (Section 4)

A number of the definitions in ISO 31000:2018 have a special meaning different to that which is used by other risk specialists that do not use the Standard. These definitions in the Standard are not based on scientific evidence and appear to be based on conjecture. The Society for Risk Analysis has compiled a glossary that reflects accepted scientific knowledge and the peer reviewed literature (SRA, 2018). The foreshadowed review of ISO 31000:2018 should consider these definitions as an authoritative source.

Issue: the definition of risk

A lack of meaning in the definition

Superficially, the definition of "risk" ("the effect of uncertainty on objectives") looks meaningful, but has been subject to criticism for its vagueness, ambiguity, and low utility for better understanding risk. In order to make sense of the definition, we all have to make assumptions that the definition has a particular meaning, with the result that the definition is interpreted very differently by different readers. This view is supported by *ad hoc* verbal surveys taken at training courses, workshops, interviews, etc. since the Standard's publication, and involving several hundred individual perspectives.

For many of us, in practice, the definition of risk can only begin to be understood if we add our own additional concepts and words to the definition (which many of us do intuitively). ISO 31000 itself has to add additional words within the body of the Standard in order to make practical sense of the risk definition. For example, "risk management … supports the *achievement* of objectives" (in: Section 4: Principles), "… customised to *achieve* objectives …" (in: Section 6.1: General), "risk management takes place in the context of the objectives *and activities* …" (in: Section 6.3.3 External and internal context), "uncertain that they will *achieve* their objectives" (in: Introduction), "explicitly address uncertainty in *decision-making*" (in: Section 5.5 Implementation, "uncertainties that can affect *outcomes* and objectives …." (in: Section 6.3.4: defining risk criteria).

ISO 31000's definition of risk has no scientific justification (Aven, 2017a), and is logically inconsistent. A test of logical consistency of a definition is to substitute any special use of a word with its own definition. In the case of the definition of risk "*effect of uncertainty on objectives*", the word effect carries its own special definition where "effect" is a "*deviation from the expected*". If this definition is then substituted into the risk definition, the result is gibberish: "*deviation from the expected of uncertainty on objectives*".

The vagueness of uncertainty

The risk definition's use of the concept of 'uncertainty' remains very vague (see "*Issue: The meaning of uncertainty*" below) and still leaves unresolved the question of how does uncertainty affect an objective? Well simply it cannot. An objective is something that is intended, aimed at, or sought after, whilst 'uncertainty' is a state of understanding.

Whilst uncertainty cannot affect the objective itself, uncertainty can affect:

- How we make sense of our 'world' and understand the range of potential options and the extent to which those options may be desirable or undesirable, and from which 'objectives' may be derived.
- How we make decisions about which of those options we would like to pursue and those that we do not wish to pursue.
- How we conceptualise the different approaches we could take in pursuit of the preferred options.
- How we understand how our environment is changing and could continue to change in the future, and how this may affect our preferences over these preferred options.
- How we determine the comparative benefits and disbenefits of pursuing different future courses of action.
- How we understand the efficiency and effectiveness of or chosen approaches in pursuit of our preferred options.
- How we determine the current and continuing future relevance, appropriateness, and usefulness of those objectives associated with our chosen options.
- How we may need to adjust our preferred options or pursue different options as our strategic and operating environments change over time.
- How we think about, design, and mobilise strategies around our preferred options (objectives).
- How we develop operational tactical plans and implement those plans in pursuit of these preferred options (objectives), in particular, which factors may enhance or diminish our chances of success.
- How performance and success is enhanced or diminished in the pursuit of purpose and objectives.
- How we monitor, measure, and make judgements about the efficiency and effectiveness of our pursuit of objectives.
- The accuracy and precision of the models and tools used in analysis of our intent and the outcomes we achieve.

Which of these potential 'effects' is considered in the use of 'uncertainty' in the Standard's definition of risk? All of them, some of them, none of them? We simply do not know, and hence are simply left to make assumptions, from which each reader of the Standard will have a different interpretation of the *"effect of uncertainty ..."*.

Uncertainty then can have an effect on how we determine our purpose and intent, and how we go about pursuing that purpose and intent. Ultimately, uncertainty affects the proficiency and accuracy of our sensemaking and decision-making that we engage in whilst pursuing successful (desired) outcomes. So, if 'uncertainty' cannot directly affect objectives, what can have an 'effect' on objectives. A change in our environment can create a hazard or threat, or other circumstances. These risk sources have the potential to interact with an organisation and generate a range of different effects, some of which will affect the design, development, pursuit, relevance, achievement of, or perception about objectives and some of which will not. The uncertainty (which influences the cognitive construction of the risk) may be about:

- The nature of the risk sources.
- The probability of and duration of occurrence of these risk sources.
- The nature and probability of interactions between the risk sources and the organisation.
- The nature and probability of the effects created by these interactions.
- The extent and probability of an effective response to these effects,
- The extent of consequences that arise following the organisation's response, and the extent of any recovery from or exploitation of these effects and their consequences.

However, in none of these cases does the uncertainty act upon the objectives directly. Interactions that could occur amongst the different factors (described by, or associated with the risk scenario) will potentially create effects that may influence the establishment or pursuit of objectives. The extent and probability of these potential interactions and effects will be uncertain to a greater or lesser degree. However, should this future potential 'event' described by the risk actually occur, then the effect will occur irrespective of any uncertainty that we have about the potential of this event and its consequences.

Whilst uncertainty is an important aspect of risk, our actions are not aimed at stopping the effect of uncertainty on objectives, but are aimed at reducing uncertainty so that we may better understand what may happen to those objectives and make more informed decisions in pursuit of those objectives.

Why focus on objectives?

We should also consider why we use 'objectives' and why these are important. Objectives fulfil two main functions:

- They are expressions of intent for creating a desired future state, and
- They can be crafted to provide a target for that intent, and a measure for that target.

It is the extent to which we can successfully achieve our 'intent' and 'desires' (outcomes) that is important, not the objectives themselves. There is also an issue that change may result in (uncertain) future unwanted effects on things other than objectives (or where objectives have not been fully articulated). If objectives are not affected, then by ISO 31000 definition this would not constitute risk. Perhaps we should be more concerned about effects on 'things of value' (Aven, 2016) than solely on objectives.

There is also the issue of situations in which multiple objectives exist. How is risk assessment affected when some of or all of these objectives conflict with each other? What happens in situations where objectives not only conflict, but are diametrically opposed or are mutually exclusive. How then do we compare and make sense of risk?

Taking this argument even further, what about situations where objectives have not been fully articulated or do not exist, or will not be formulated until sometime in the future? Under ISO 31000's definition, in such situations we would be unable to consider risk, until such a time as an objective was articulated. This would also mean that it would not be possible to assess risk in the early stages of strategic thinking, as objectives would not have yet been formulated. In a practical sense, 'integrated' risk assessment should help to formulate these objectives, thus creating a 'chicken or egg' paradox, which comes first? The only way that 'objectives' can be used as a general definition of risk, one has to postulate that in any activity or situation there is always the objective of minimising harm and maximising success, even if that objective is implicit, unrecognised, not articulated and not consciously agreed to by someone. In which case, risk cannot 'exist' in the absence of someone that could be affected by the circumstances described by the risk.

The inclusion of "objectives" as a key aspect of risk management owes its existence to the philosophy of the aging "management by objectives" movement. However, this has also shown to be a flawed

philosophy[26] and has been subjected to criticism (Cardona and Rey, 2022; Burnham, 2016; Kyriakopoulos. 2012; Kaplan 2010; Bergman and Klefsjö, 2002; Deming, 2000; Dinesh and Palmer, 1998; Jamieson, 1974). Management by objectives can fail to achieve its own 'objectives' because this focus can result in other important aspects of the organisation being ignored.

Obviously, if something (uncertainty, an event, it doesn't matter for this part of the discussion) does affect objectives, we can determine the nature and magnitude of the effect, for example as 'impacts' or 'consequences'. However, how can we make any estimate of risk if those 'consequences' are undefined (Aven, 2017a), or where the risk management process internally defines those consequences, rather than them being defined as a strategic analysis of the objectives themselves.

The current definition of risk is sufficiently vague and sufficiently flawed to warrant its exclusion as the basis for the whole of risk management which comprises ISO 31000.

An absence of logic

The definition of risk in ISO 31000 has been and continues to be the subject of much debate. Let us, for the moment ignore all of the preceding commentary above, and assume that the existing definition of risk is 'correct': i.e., that risk is "the effect of uncertainty on objectives".

The logical premises that are created from this definition are:

- An "effect of uncertainty" means that uncertainty exerts an effect on objectives.
- To exert an effect, that effect must arise from the uncertainty, or arise when uncertainty interacts with the objective.
- The effect is therefore dependent upon the uncertainty.
- If the uncertainty changes, then the effect should also change.
- If the uncertainty is reduced, then the effect should be reduced.
- If the effect is reduced, the risk is reduced.

The logical (but false) conclusion to this is that if one reduces uncertainty, then the risk is reduced, irrespective of what other changes are occurring in the environment. Therefore:

- If more data is gathered as input into a risk assessment, then uncertainty is reduced, and the risk is reduced.
- If that data is analysed to produce information, then uncertainty is reduced, and hence the risk is reduced.
- If that information is used in risk evaluation, then the risk is further reduced.

To illustrate the fallacy, if one takes a hypothetical risk of a mechanical failure on a single engine aircraft on take-off resulting in a crash into the ground, then the sole action of assessing that risk will reduce the uncertainty and reduce the risk. By logical extension, if enough analysis is conducted, then one could get close to near certainty, and the risk would be reduced to near negligible. But has the risk assessment actually changed the presence of a design error or a fault due to poor maintenance of

[26] To quote the 'father' of the whole philosophy of management by objectives, Peter Drucker, "**Management by Objectives works if you know the objectives, 90% of the time you don't**" (Ghicajanu, 2008).

the engine? Or the number of flights before the failure occurs? Or the ability of the pilot to get back on the runway safely?

So how does uncertainty have an effect on objectives?

In both qualitative and quantitative risk assessment, the value of risk is often expressed as a range. If enough analysts performed enough analyses of a risk, it would be possible to narrow that range to a value, with a small degree of error above and below that value. If one then looks at a single assessment of that risk, the error (for both consequence and probability) would be greater than for the combined assessment. If that single analyst gathered more observational data and used more sophisticated analytical tools, they would reduce uncertainty and would be able to reduce the level of error in their measurements and outputs (Figure 1). Thus, as more data is collected, uncertainty is reduced and the amount of error about consequence and probability is reduced. Analysing that data further reduces uncertainty (and error), the level of reduction depending upon the choice of analytical tools. With a further reduction in uncertainty is achieved during evaluation. Again, reducing the uncertainty can certainly reduce the error in measurement (improving the precision and accuracy of our understanding about risk) would not necessarily change the value or level of that risk[27].

It could therefore be concluded that changing uncertainty reduces the error in risk measurements, and therefore uncertainty 'effects' objectives by changing the accuracy of measurements of the effects upon those objectives, but does not affect the objectives themselves. Therefore, the "effect of uncertainty on objectives" is not a risk, but a change in the error associated with measuring that risk, which by extension means that the definition of risk lacks logical proof.

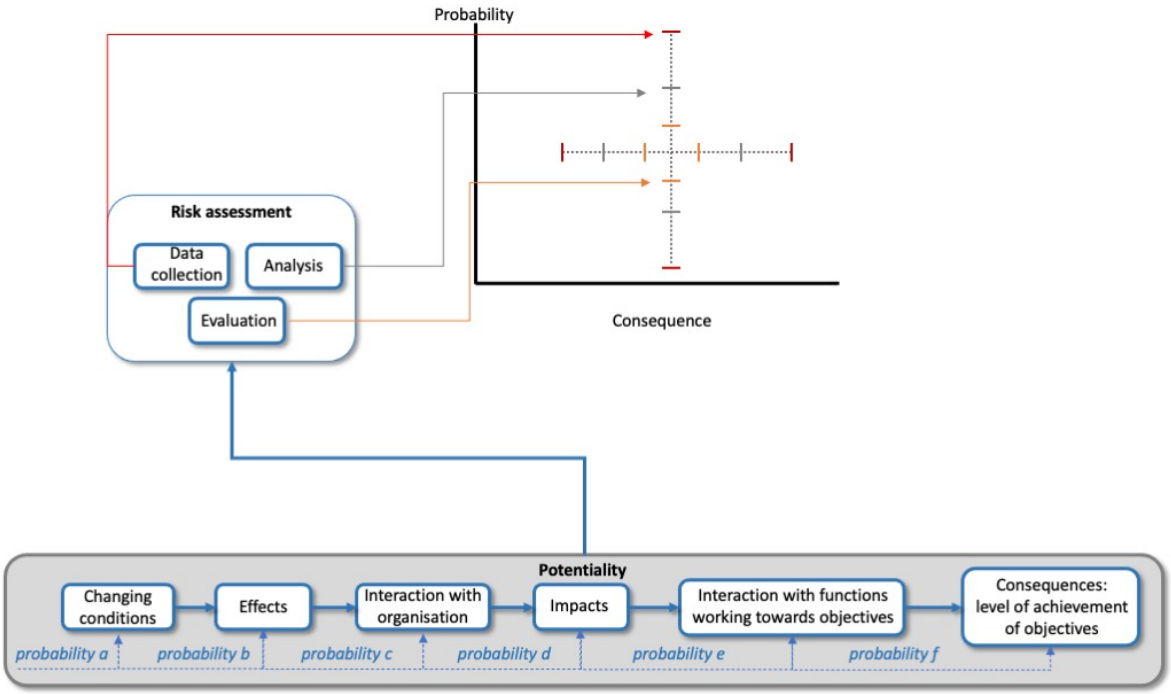


Figure 1: The effect of uncertainty on objectives, an error reduction model

[27] However, with reducing uncertainty, if that increased knowledge is used to inform decision making, then a meaningful change in the nature and amount of risk could be achieved.

Resolution
The conceptualisation of risk and its definition requires considerably more research and thought in order to undertake any meaningful revision of the Standard.

We do not wish to presuppose these deliberations, or to propose the following as acceptable replacements for the current definition, but merely provide these as examples of ways in which a risk management definition could evolve;

a) *"The potential for a future set of circumstances to occur that have an effect on the pursuit and nature of organisational success"*[28].

   Note: Where that potential is uncertain and is expressed through measures or estimates of the probability (or likelihood) of the effect.

b) *The potential future effect of conditions, events, and decisions, on something of value.*

Notes:
i) Where potential future effects are uncertain but can be estimated or measured.
ii) Conditions, events, and decisions are sources of risk, and may have existed in the past, currently exist, or may exist in the future.
iii) Where something of value may be personal, shared, group, organisational, communal, or societal.
iii) Where value may be tangible, intangible, or assumed.

This then leads to a consideration of what do we mean by uncertainty?

Issue: is ISO 31000 uncertain about the meaning of uncertainty?

The concept of 'uncertainty' is core to the current definition of, and fundamental understanding about the nature of risk. However, 'uncertainty' is not defined and is otherwise scarcely considered in ISO 31000:2018 (appearing in only 4 short generic statements in the whole document). For something that is so crucial to the whole conceptualisation of managing risk, its relative absence in the Standard, is perplexing and constitutes a critical flaw. This Whitepaper discusses uncertainty in more detail in its examination of 'risk criteria' below.

Resolution

The next version of ISO 31000 has to establish a very clear concept of 'uncertainty', establish its relationships with risk, and with achieving (or not achieving) organisational success.

[28] Note that the first definition, specifically limits 'risk' to an organisation, since the scope of ISO 31000 currently limits risk management to an organisational context. Such a definition also removes the tension between the followers of ISO 31000 and practitioners in other domains, freeing up (without conflict) these other domains to define risk as they wish for their own specific context. However, there is still an argument for developing a Standard that is flexible enough to deal with a wider application of risk outside of just an organisational context.

Issue: definition of risk source

A risk source is defined as something which "has the potential to *give rise to risk*". What does this actually mean? The term "give rise to" can be interpreted as to cause a situation or event to occur. With risk we have a socially constructed model or scenario which describes a potential future situation. Common 'risk sources' are hazards and threats, they do not "give rise" to a risk but they can "give rise" to interactions and effects on something. They are the potential factors which can interact with an organisation or system and can "give rise" to a range of potential future events and impacts. It is from our understanding about how these risk sources could "give rise" to future situations that we then construct and describe as risk. What actually 'gives rise' to risk are the very different factors that affect our perception and cognitive construction of that risk.

Resolution

ISO 31000 is scattered with allusion to risk as some tangible 'entity' that has its own independent existence, rather than as a cognitive construction used to describe a set of relationships (actual and potential). Words have power, and a Standard has to be exceptionally careful about the words it uses to describe key concepts. The inappropriate use of language in the current and prior version of the Standard has resulted in the use of inappropriate language by practitioners, conceptual misunderstanding, and the adoption of inappropriate practices. The revision of the Standard has to carefully consider every word used to ensure there is no vagueness, ambiguity, or other scope for unintended interpretation.

Issue: the definition of risk management

The definition of "risk management" in the Standard appears to be a technically incorrect use of the term "direct and control…", a term which is more commonly applied to 'governance' than to 'management'. In contrast 'management' would involve making decisions and taking actions aligned with the direction and control exercised by the governing body[29]. It appears that the definition of "risk management" used in ISO 31000 applies more to a concept of 'risk governance' than it does to actual management. Unfortunately, the Standard almost completely ignores the concept of risk governance[30].

Resolution

The definition of risk management needs to better recognise the difference between 'governance' and 'management' and specifically needs to account for the overarching differences between 'direction, oversight and control' (risk governance[31]), and the procedural conduct of risk management. The concept of 'risk governance' is discussed in more detail below.

[29] Whilst recognising that a governing body also takes decisions about governance and setting strategy.

[30] Because ISO 31000 makes no effort to explain 'risk governance', and the term is used widely outside of ISO 31000, there is the potential for significant confusion amongst practitioners. Alternate views do exist that 'risk governance' as well as oversight includes decisions about strategy made by the governing body and top management, whilst others view the strategy elements as part of 'risk management'. Thus, there is no current agreement if 'risk governance' is a part of 'risk management', or if 'risk management' is the operationalisation of overarching 'risk governance'.

[31] Agnese and Capuano, 2020.

The section on principles

The principles are perhaps the most important inclusion in ISO 31000:2018, in its evolution from AS/NZS 4360: 2004. They are also, unfortunately, perhaps the parts of the Standard most ignored and disregarded by practitioners. Based upon discussions in training courses, workshops, and conferences, and involving many hundreds of 'risk practitioners', it appears that the 'principles' are given little more than lip service in many organisations' risk management approaches. That is apart from a few more 'mature' practitioners, for which the principles provide a foundation and ongoing guidance for their activities.

The inclusion of 'principles' into ISO 31000 was a good step in the ongoing development of the Standard. The core of the principles is insightful and provide a set of foundational criteria upon which the design and sustainability of an organisation's risk management approach can be undertaken. These principles also provide a core suite of criteria on which the performance of the risk management approach can be monitored, measured, judged, and assured.

However, the Standard's section on principles is often highly generic and vague, and is based on some prominent assumptions that have yet to be validated, and conjecture that requires further exploration.

Resolution

It must also be remembered that, although the principles appear to make sense intuitively, there is a lack of supporting evidence for many of the claims that the Standard makes about these principles. In the forthcoming revision the following questions need to be resolved about the principles:

- How do we know that these are the most important principles? Are any of the current principles less important, or relevant only to specific contexts or applications of risk management, and hence could be removed or substituted?
- How have these principles been validated?
- Are the principles fit-for-purpose now and for the foreseeable 'tenure' of the next iteration of the Standard?
- Do they make sufficient sense that they can be meaningfully applied without additional explanations? Are they sufficiently clear and understandable to effectively guide the design, operation, and evaluation of an organisation's risk management arrangements?
- Are they sufficiently durable over the expected range of contexts across which they may be applied?
- Are they sufficiently comprehensive to encompass the most important and relevant guidance for establishing and maturing risk management?
- How do we know that no other important principles have been omitted? For example, any of the following could also be included into the Standard as equally, if not more important principles compared with the existing principles (and there are many more that could be considered for inclusion):
    - Scientific evidence: Effective risk management is based upon sound scientific evidence (Aven, 2019).
    - Contestable information: Analysis of risk and its outputs, and risk informed advice is contestable, and multiple valid information sources are sought to ensure that risk information is fit-for-purpose.

- Validated assumptions: Effective risk management recognises that assumptions underpin all perceptions, interpretation, and decisions, and that these assumptions need to be surfaced, challenged, and validated.
- Conceptual and technical limitations: All risk management arrangements, methodologies, tools, and techniques have their limitations. Effective risk management recognises these different limitations, and makes informed choices about which approaches are optimal. Such choices are based upon the nature of the context, the objectives for risk management, the nature of the available data, and the competencies and experience of those involved in risk management.
- Evidence -based decision making
  Decision-making is based upon relevant evidence (validated data and information), which includes being 'risk-informed'. Since, risk information is supplemented by other types of analysis and sources of information, effective decision-making is 'risk-informed', rather than 'risk-based'. Using the term 'risk-based' implies that decision-making is limited solely to the risk information product[32].

Issue: missing the principle, a lack of attention and understanding?

One of the tests of understanding about ISO 31000 we regularly undertake in training is to simply ask risk practitioners two questions:

- What are the principles?
- How do you apply the principles?

We have found that many 'risk practitioners' can only remember a couple of the principles in the Standard, and even then, they can be pretty vague about these principles and how they are applied.

The Section on principles in ISO 31000:2018 is fairly prominent and has its own figure summarising these principles. Why then are they not more strongly considered and featured in organisational risk management approaches? Why do many 'risk practitioners' pay them such scant attention?

Despite the inclusion of the principles in Figure 1 and the arrows connecting both the 'framework' and the risk management process, the section on principles stands on its own, isolated from both the framework and process. A single sentence in the introduction to the principles provides the only clue to the importance of this integration. The very way in which this introduction is written as a collection of generic statements (without real explanation) probably encourages many readers to 'gloss over' this introduction without recognising its importance.

In reality, the principles are a core part of the risk management framework, but this integral nature is lost by Figure 1 in the Standard which reinforces the conceptual isolation of the principles This diagram strengthens a cognitive dissonance between the principles and the process, and by mistaking an aging improvement process for a risk management framework.

[32] See Kumah et al, 2019, and Epstein, 2011; 2009, for studies demonstrating the increased efficacy of evidence-informed approaches compared with evidence-based approaches.

Resolution

The principles are a core driver and enabler of the risk management framework, and an essential component of the risk management process. Figure 1 needs to be redesigned to clearly show what a risk management framework comprises (and it should be so much than a tired old PDCA cycle[33]), and that the principles are an essential part of this framework. Almost all governance systems rely on the establishment and acceptance of a suite of principles. By reimagining the framework as the structural element of a formal risk governance system (see below), the principles will be given heightened prominence and will help to better drive their adoption.

Issue: on the nature of principles

Another possible reason for the low recognition of the importance of the principles is that they are written as fairly vague generic statements, with little guidance about what they mean in a practical sense. The absence of supporting evidence for some of the principles must also raise questions about:

- Are the current 'principles' in the Standard actually principles?
- Are all of the current principles appropriate?
- Are they written as understandable and useable principles?
- Are there other concepts that are either missing from the list of principles or that should be incorporated to expand our understanding of each of these principles?
- Should other concepts/principles be additional to the list, or should they replace one or more of the current principles in the Standard?

Although there are multiple different definitions of a 'principle', most carry the concept of a basic *truth*[34], that guides a flow of reasoning and forms the basis for other truths and beliefs, which by definition means that a principle is based upon fact. This should require that any principle promoted by ISO 31000:2018 must be supported by evidence, not just that it feels intuitively appropriate. The Standard clearly states that "effective risk management" requires these principles. The 'truth' and evidence that supports each of the principles is considered for each individual principle (below).

The purpose of risk management

Curiously, the list of principles does not include the 'creation and protection of value', which instead is regarded as the *purpose* of risk management. It is arguable if this is a realistic purpose, as the real purpose of risk management is to provide a systematic approach for managing risk. Managing risk may contribute to creating and protecting value, for example by informing decisions about reducing losses, pursuing opportunities, and realising benefits, etc. In this respect, managing risk assists other functions (Finance, Security, Health and Safety, Procurement, Insurance, Operations, etc.) in making decisions and taking action that protects things of value to the organisation from harm or loss. Similarly, managing risk may also assist other functions in making decisions that create value (for example, Customer Relations, Product Development, Brand and Marketing, etc). In other words, risk management itself neither protects nor creates value, rather a whole range of other functions provide

[33] See the first issue in the Section on 'Framework' below for a discussion on this PDCA cycle.

[34] Something which can be proven or validated, something which is supported by convincing evidence.

this value, supported by the way in which *risk is managed* not necessarily because a formal process called *risk management* is occurring.

Is there any evidence that would support the Standard's claim for the creation and protection of value? At first glance it would appear that there are numerous examples where organisational value is associated with the management of risk (Rampini et al, 2019). For example, some insurers may reward organisations with reduced premiums for having recognised risk management approaches in place. However, if we actually look closely at the published evidence, a more nuanced picture begins to emerge.

Across the multiple publications supporting risk management's protection and creation of value, a majority, especially in the non-academic literature, simply repeat this popular mantra without actually reporting any verifiable evidence. There is some compelling evidence that 'risk management' in the financial sector may indeed contribute to measurable value. Although in this respect, this is using sophisticated financial risk instruments beyond the knowledge of the average 'risk practitioner' outside of the financial sector, and does not rely upon using ISO 31000 (CFI Team, 2023; Leo et al, 2019; Kanchu and Kumar, 2013; Woods et al, 2008). The evidence for risk management's contribution to the protection and creation of value outside of the financial sector is far less compelling. Much of the supportive evidence that has been published is either based on theoretical modelling (rather than real-life experience), or shows correlation rather than causation (Willumsen et al, 2019; dos Santos et al, 2017; Ittner and Keusch, 2016; Schrödl and Turowski, 2014, FM Global, 2012; Kraus and Lehner, 2012). It is probable that risk management *contributes* to protecting value, however, the case for value creation is far weaker.

Even if we accept the premise (based on evidence of correlation rather than causation) that 'risk management' contributes to both value protection and creation, this still does not make the case that using ISO 31000:2018 protects and creates value. That are no robust scientific studies, to date, that show any strong causal relations between the operation of the Standard and the protection or creation of value for an organisation[35]. Specific 'evidence' for the role of ISO 31000 remains firmly in the conceptual and theoretical (Alijoyo and Norimarna, 2021).

This apparent lack of strong evidence for the value contribution of formal risk management, is further demonstrated by independent research surveys. These demonstrate a powerful perception amongst a majority of senior executives that risk management (in general) contributes little to strategic value – in over 80% of organisations surveyed (Beasley et al, 2019).

If not value, then what is the purpose of risk management?

The purpose of risk management is not to create and protect value. The actual purpose of risk management is to provide mechanisms (frameworks, procedures, processes, tools, and techniques) to better address uncertainty and its influences on sensemaking and decision-making *associated* with those activities that create and protect value. For example, if we consider what are the key things of value in an organisation (such as sales and revenue, reputation and brand, people capability; integrity, fit-for-purpose products and services, market share; employee health and wellbeing, and job satisfaction), then risk management does not create this value, nor does it directly protect it. Risk management is just one cog in every large 'system', with risk management making a contribution to those other parts of the system that do create and protect such value.

[35] Most studies showing correlation between risk management and improved organisational performance looked at methodologies other than ISO 31000, or were silent about the methodology in place.

Resolution

Our original starting point was that 'create and protect' should have been accorded the status of a 'principle'. However, given that a principle is a foundational truth, and the lack of robust evidence supporting such a foundational truth, then perhaps 'create and protect value" should neither be the purpose or principle of risk management. Rather it should be the ultimate desired outcome for effective risk management. That is, we can make no valid claim beyond: "*effective risk management should contribute to the protection and creation of value*".

i) Principle – "Integrated"

Under the heading of "Integrated", the Standard states that "*risk management is an integral part of all organizational activities*". Unfortunately, it appears that the Standard is confused, believing that these two words carry the same meaning. 'Integrated' and 'integral mean' mean two very different things. 'Integral' means to be an important or vital part of something, if something that is 'integral' is missing or removed, then functionality will be lost. Integrated, on the other hand, means linked, coordinated, or combined with something. For example, this could convey the meaning that a separate risk management process is coordinated with a separate strategic planning process. The two processes interact and they are 'integrated', but neither one is an essential element of the other.

This then raises the question, should this principle be about being 'integrated' or about being 'integral'?

The concept of 'integrated' appears to be misunderstood by many risk practitioners, and is highly contested by some. We have run frequent surveys of clients, and in workshops, training courses and at conferences to gauge how risk practitioners interpret the concept of 'integrated' and have come away with almost as many different answers as the number of people we have asked. Their responses range from having completely standalone risk management process that provides data to another organisational function, through to a sensemaking capability that is strongly embedded in the core functions of the organisation.

Any examination of organisations within any sector would be expected to show a spectrum of levels of risk management 'integration', from an absence of any formal risk management[36], to low integration, up to highly embedded in some organisations (Figure 2). However, we have found no robust evidence that demonstrates a convincing causal relationship between the level of 'integration' of an ISO 31000 based risk management approach and strategic or operational performance[37]. Similarly, there are numerous anecdotal accounts globally, where risk management functions have been eliminated from organisations or have been restricted to compliance and assurance activities, with no apparent impact on strategic and operational outcomes.

[36] We are aware of one particular highly successful company with a global brand that has been prominent for decades, and which does not have an identified risk management function, does not produce separate risk management reports for management or the Board, and does not employ any specific risk management professional. However, managing uncertainty and risk is an integral capability and is embedded and embodied within all parts of the organisation.

[37] Much of the published literature does show a correlation between the presence of formal 'risk management' and the claims history of some organisations. However, such performance could be a result of a whole host of factors, and the presence of risk management may be coincidental, a reflection of organisational maturity and capability. The causal relationships may very well reside in how risk is managed generally with increasing organisational maturity, rather than the contribution of a formal risk management function.

Conversely there is a significant body of literature which demonstrates substantial organisational impairment and disruption when the *management of risk* is not *integral* to critical decision-making and other core activities (Gibson and Gibson, 2023a, Gibson, 2020).

It therefore appears that making the management of risk 'integral' to core functions is more important that just de facto trying to achieve some form of nebulous 'integration' of the risk management process. How we need to go about establishing risk management as an integral part of such core functionality will in large part determine the level of 'integration' required. As with many other aspects of risk management, this will largely be determined by the context.

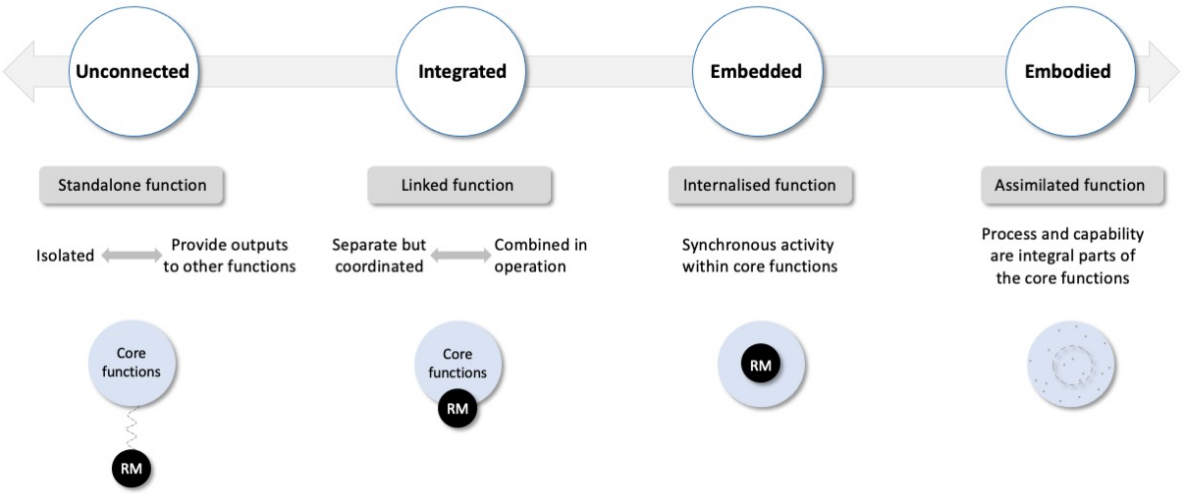


Figure 2 Spectrum of incorporation of risk management[38]

An example of the benefits of moving to an embedded /embodied management of risk is provided by the transformation away from restrictive linear strategic planning approaches (Martin, 2014; Barrows 2009; Rowland, 2006; Chussil, 2005; Liedtka, 2000) and towards more interconnected and unified 'strategic thinking' and 'strategic leadership'[39] concepts (Asoee, 2021; Lonča, 2017; Toma, et al, 2016; Bouhali et al, 2015; Salih and Alnaji, 2014; Nuntamanop et al, 2013; Fairholm and Card, 2009; Heracleous, 1998). The limitations of this old 'integrated' thinking about risk management reinforces problematic strategic planning, where risk management is often bolted-on to provide an input at the start of planning (as part of horizon scanning) and at the end as an input into testing of the draft plan.

Strategic thinking, strategic leadership, and strategic management approaches more readily demonstrate where risk management can be readily *embedded* into the whole strategy development and implementation, rather than just 'integrated' as a bolt on process. Similarly risk management can be embodied within other organisational capabilities, simply as the way that these functions operate every day.

[38] 'RM' is the diagram refers to 'risk management'.
[39] Where 'strategic planning' is just one integral element of the overall unified approach.

Resolution

It can be strongly argued that in order to deliver maximum benefit to an organisation, risk management needs to be not 'integrated', but rather 'embedded'[40] and '*embodied*'[41]. For example, consider the 'strategic planning' example above. In the last few decades, in the face of increasing volatility, novelty, complexity, and resulting uncertainty, many organisations have moved away from a sole reliance on rigid strategic planning, to a more dynamic and explorative strategic management approach. Such a strategic approach can involve a suite of 'nested' processes (Figure 3).

As uncertainty will be present across all of these nested processes, and will influence strategic decisions and the pursuit of strategic objectives, then risk management will need to be an ongoing activity across all of these activities:

- *Strategic thinking processes*, including:
  - understanding and analysing the problem space;
  - exploring interdependencies, interactions, and vulnerabilities, and the way in which they could change and influence the future landscape;
  - considering the manner in which new challenges and opportunities could emerge; etc.
- *Strategic design processes*, which are increasingly using human centric design thinking approaches to better explore and understand stakeholder needs and potential solutions (Graf, 2021; Vuillermin and Huck-Sandhu, 2021; Diderich, 2020; Knight et al, 2020; Stevens et al, 2008) and red teaming techniques (Neal-Boylan and Rotkoff, 2021; Zhou and Sun, 2020; Longbine, 2008; Sandoz, 2001), which can be extended across the whole strategic management approach in order to surface and challenge underlying assumptions.
- *Strategic formulation and planning processes*, in which decisions are made about the agreed strategic objectives, and the other decisions, tasks, resources and time requirements, that are required to achieve those objectives, are established and documented.
- *Strategy implementation processes*, through which the tasks, resources, and processes are mobilised, and deployed.
- *Strategic governance processes*, by which the implementation of strategies is directed, controlled, overseen, monitored, evaluated, assured, and reported upon.

[40] Embedded - firmly and deeply situated within something.
[41] Embodied - essential integral constituent part of something



Figure 3: Risk and strategic management - an embedded whole

ii) Principle – structured and comprehensive

This principle is exceptionally vague in the Standard, and is open to wide interpretation of meaning.

The meaning of "structured and comprehensive"?

What exactly does "structured" and "comprehensive" actually mean? Does 'structured', in this context[42], refer to:

- A rigid framework that is applied consistently across the organisation?
- A rigid process that is applied consistently across the organisation?
- An approach that is strictly governed by rules and requirements?
- Arranged and undertaken according to a defined plan[43]?
- Following a predetermined pattern?
- Organised to show the relationship between the parts?
- Organised organically so that it resembles a living organism, or according to organisational reporting lines?
- Comprising a sequence of discrete steps?

[42] Remember 'structured' is contributing to consistency and comparability.

[43] This is closest in meaning to the general dictionary definition of 'structured', and if this is the meaning, why not just say a planned approach.

Similarly, what does 'comprehensive' mean in this context, does it refer to:

- Having all possible steps included?
- Using all possible analytical tools and techniques?
- Involving all parts and people within the organisation?
- Includes all hazards and threats?
- Gathers and analyses all available information?
- Considers all aspect of strategy and operations?
- Involves all functions and levels of the organisation?
- Considers all controls and their efficiency and effectiveness?
- Examines and explores all vulnerabilities?
- Surfaces and challenges all assumptions?
- Examines all interrelationships and interdependencies?
- Lists all risks?

The principle is so vague, that to make any meaning of it the reader has to add their own interpretation. With individual perception, interpretation, and application, comes variability. How then does this align with the aims of "consistent" and "comparable"?

The meaning of "consistent" and "comparable"?

We have been unable to find robust published research that shows any such consistency and comparability of results achieved by applying the ISO 31000:2018 Standard. In fact, the reverse appears to be the case, with multiple publications criticising the Standard in this respect. It seems likely, from anecdotal evidence[44], that many users of ISO 31000 have established qualitative risk management approaches that have in-built inconsistency in the way that analysis is conducted and interpreted.

ISO 31000:2018 does not distinguish between qualitative and quantitative approaches, but de facto promotes their equal application for risk assessment[45] and in doing so directly conflicts with the very ideas of "consistent and comparable". It is increasingly accepted that qualitative methodologies are so subjective that they carry inherent inconsistency (Gibson and Gibson, 2023; Lengyel et al, 2023; Blum, 2020; Grabel, 2020; Maze, 2018; Gerstein et al, 2016; Rozell, 2015; Tebehaevu, 2015; Shang, 2014; Zhou and Leung, 2012; Emblemsvåg and Endre Kjølstad 2006; Karabacak and Sogukpinar, 2004). Analyses using exactly the same data sets, but conducted by different analysts, commonly yield significantly different results. Furthermore, even the same analyst using identical data sets, but at different times can again produce different results (Hubbard and Seiersen, 2017).

Quantitative techniques, generally, will be more consistently applied and will produce more comparable results. However, quantitative analyses are also subject to a wide range of biases that can produce inconsistencies and reduce comparability of results.

[44] From personal communications from various risk professionals to the authors of this Whitepaper, and the authors' personal observations of widespread risk management practices.

[45] This Whitepaper is not trying to make the case that quantitative techniques are always superior to qualitative techniques. The authors believe that there are situations where a qualitative assessment can provide a different and sometimes more valuable insight into risk than some commonly used quantitative techniques. However, taking the limited view of just rating and ranking risk, then quantitative techniques will tend to be more accurate and precise, and be more consistent across time and across different analysts.

Of matrices and heat maps

Furthermore, it appears that ISO 31000:2018's similar silence on the problematic use of risk matrices and heat maps, has done nothing to dissuade many practitioners, consultants, and software developers from continuing to promote poor practises in this respect. Informal surveys indicate that the vast majority of the users of ISO 31000:2018 are using qualitative assessment techniques, of which almost all are using risk matrices and heat maps of some description.

In making this point we are not saying that all applications of risk matrices are terrible and should never be used. There are some circumstances were these matrices can be useful (and at times we have also used matrices). However, the vast majority of risk matrices are poorly calibrated, largely unvalidated, rarely adjusted to changing contexts, and their users have little appreciation of their limitations and hence will fail to make any accommodation for these problems (Thomas et al, 2018; Cox, 2008). Whilst many of the criteria on which the matrices are based are often vague and hence open to substantial variability in interpretation, and are commonly poorly aligned with the prevailing context. The problems with risk criteria will be discussed in more detail later in this Whitepaper.

Inconsistency – an inherent problem?

ISO 31000:2018 claims to be founded on a principle of "consistent and comparable results", yet the vagaries and linearity of the described approach does little to ensure that the analytical methodology itself has sufficient consistency and comparability in its design and execution. These problems of consistency and comparability are further compounded by the Standards complete omission of mention of the essential need for calibration. Without robust calibration, risk methodologies, risk criteria, risk matrices, appetite and tolerance values can easily be rendered meaningless. Although uncommon in ISO 31000 based methodologies, calibration is more routinely applied in other risk analysis domains (Connors and Large, 2023; Hubbbard, 2020; Van Hoorde, 2014; Borgert et al, 2012; Pressman and Flocton, 2012;Rael, 2012; Calder and Schwehr, 2009). Even where calibration of the analytical tools is undertaken, substantial variability and error will still be introduced if those involved in the analysis are themselves not calibrated (Sivitski and Põodra, 2021; Notebaert et al, 2016).

Resolution

The intent of the Standard to remain non-prescriptive is strongly supported. However, in doing so it has allowed a proliferation of misunderstanding and poor practices. In the revision of the Standard, careful consideration should be given about the provision of advice on the relative merits of quantitative and qualitative risk assessment methodologies. This especially needs to include advice about the need to understand the limitations of different approaches and address some of the myths that have grown around certain practices (for example, the mathematically invalid practice of trying to multiply out linear nominal and ordinal scales on risk matrices to derive a risk rating, when input values are exponential). Consideration should also be given in the revision to including guidance on both the calibration of risk assessment tools and of people contributing to the process.

iii) *Principle - Customised*

This is perhaps one of the most understandable of the principles, although it is still written in such an obtuse and abstruse way that it seems almost purposefully worded to confuse the reader. The reader is still left making assumptions in their attempt to derive meaning.

Our interpretation of this principle is that the risk management approach has to be customised to work effectively within the context that it is to be used. This may mean that, on changing to a different context (e.g., from one organisation or business unit to another, or in a context that is changing), the overall risk management arrangements may need to be redesigned. It may mean that looking at different forms of risk (e.g., routinely encountered risk compared with high consequence-low likelihood risk) may require different risk assessment processes, tools, and techniques. Or it may require that risk assessments conducted at different levels of the organisation (e.g., those conducted as part of strategic management compared with those associated with a project) need to have different risk criteria in terms of scale, value or type.

Resolution

This does naturally raise questions about a direct conflict between such a 'customisation' principle and the 'consistency' and 'comparability' principle. Whilst such a conflict can be addressed, the Standard is silent about both the need for such consideration, and guidance on how the conflict between 'consistency and comparability' and 'customisation' can be achieved.

iv) Principle: Inclusive

Another almost clearly written principle…almost.

The way in which this section is written raises a number of questions:

- What does the Standard mean by 'inclusive'?
    - just who should be considered,
    - to what extent should inclusivity be pursued?
    - how are decisions on inclusivity to be made, and by whom?
- What does 'appropriate' mean in the context of this principle?
    - what does inappropriate look like?
    - Are there certain types of 'appropriate' stakeholders that should usually be considered, and other types of stakeholders that should automatically be excluded?
    - What criteria should be applied to help make decisions about the appropriateness of stakeholders for inclusion?
- What does timely mean?
    - does this refer to the timing of stakeholders' involvement with respect to the different activities of the analysis?
    - relative to the changing context?
    - with respect to the currency of their knowledge?
    - or with respect to their contribution to decision-making based on the risk analysis?

Again, we need to make a whole range of assumptions in order to interpret this principle.

Whilst it is true that seeking diverse perspectives can provide a richer data set for analysis, can help to generate different insights that might not have otherwise been the case, and can be less subject to the effect of individual biases (Mercier and Landemore, 2012; Jackson et al, 1995). Involving too many

stakeholders or obtaining too diverse a range of inputs can lead to data overload, excessive noise[46], and confusion.

Involving diverse stakeholders will also introduce further variability into analysis, since they all come with their own different and unique mix of ideologies, perceptions, biases, and intents. Even just restricting stakeholder involvement to acknowledged 'experts' can be problematic in its own right.

There are numerous studies that show that the performance and relevance of 'expert' involvement is often lower than expected (Baur 2022; Robinson et al, 2022; Morgan 2014; Burgman et al, 2011; Charness and Tuffiash, 2008; Chi, 2006; Kardes, 2006; Ayyub, 2001; Sperling, 2000; Fishoff et al, 1982; Kahneman et al, 1982). The issue is therefore not to 'cast a wide net' to include multiple stakeholders just for diversity and inclusion's stake, but rather to select stakeholders on their context specific knowledge, experience, and involvement in that context. The involvement of different types of stakeholders may be required at different times throughout risk management activities.

Even in situations where 'appropriate' stakeholders are included, say as experts inputting into risk analysis, there can be significant biases and errors in their contributions, especially if they have not previously participated in some form of calibration (Hubbard, 2020). Care also needs to be taken where including diverse stakeholders results in strongly conflicting information, which can create problematic analysis and adverse impacts on creativity (Friedrich and Mumford, 2009). To gain the benefits of involving diverse stakeholders requires careful stakeholder analysis, engagement and management, which are other concepts that are largely ignored by the Standard.

Inclusivity for inclusion's sake is no guarantee that this principle's aim will be achieved, the reverse may be more commonly the case where stakeholder inclusion is not carefully planned. What is required is a determined activity to include those stakeholders that can make the best contribution to the specific risk management activity. Whilst acknowledging that different stakeholders may be more valuable as risk management proceeds and different data requirements and different perspectives emerge.

Resolution

This principle is often interpreted by practitioners to mean that a wide selection of stakeholders should be involved in risk management. However, not all stakeholders are equal in the extent and relevance of their knowledge, experience, and cognitive capabilities. The important principle is that only those stakeholders that can contribute something of value should participate in risk management[47]. This does not necessarily mean that only experts or those that can contribute data should be included. Sometimes 'adding value' also means involving stakeholders where their acceptance and understanding is required in order to support the risk management efforts, to subsequently commit to progressing necessary risk treatments, or that may be affected by or be resistant to risk management outcomes.

Such a principle cannot just be simply implemented, there needs to be mechanism for identifying suitable stakeholders, evaluating the contributions that these stakeholders can make, engaging with and managing their participation in activities. It is also not just the value that individual stakeholders can bring to risk management, but also additional value that can be created by their interactions with each other.

[46] To the extent that valuable signals are lost or obscured.

[47] This also includes considering involving those stakeholders that can influence or be affected by the risk management outcomes.

v) Principle: Dynamic

This principle does earn a small round of applause, for unlike the previous principles, the 'dynamic' principle does provide a short explanatory rationale, an essential element as the principle itself is fairly general and largely uninformative.

It is also arguable if some of the claims made by this principle are actually accurate and can be substantiated. How does risk management actually "anticipate, detect and acknowledge change"? These are all attributes of people, not of a framework or of processes. The risk analyst, or one or more stakeholders may anticipate future change based on data that has been gathered prior to any risk analysis (e.g., through various surveillance and monitoring activities that are not conducted through any 'structured risk management'). Alternatively, such anticipation may occur because of a 'risk practitioner's' insight that emerges during analysis, or may arise in decision makers using information outputs from risk management. Risk management may contribute or help facilitate anticipation, but risk management itself is not anticipative, only people can anticipate[48]. Similar arguments also hold for the concepts of "detects", "acknowledges", and perhaps "responds" in the principle.

Then there is the issue of the concept of "dynamic" as the title of this principle. The word dynamic is used to convey multiple subtly different meanings in different parts of the Standard, in reference to the context, to human behaviour, and to the risk management process itself. The word seems to be used to variously mean, changing, modifying, turbulent, and variable in different parts of the Standard. With respect to this specific 'principle', there are two possible considerations for thinking about risk management in terms of being "dynamic':

- 'Dynamic risk analysis'[49] is a common tool used for decision-making in volatile and highly uncertain contexts (Villa et al, 2016), such as those experienced by high hazard industries and emergency responders. 'Dynamic' in this sense means that because the operating environment is changing (volatile or turbulent), there is a continuous risk assessment occurring so that adverse changes in the operating environment are immediately understood and countered.
- 'Dynamic' where the context is changing such that the risk management process itself may need to be adjusted and adapted to better align with the change. Also, that the extent, significance, and rate of change, may invalidate earlier data and analyses, or introduce new factors for consideration, to the extent that a risk assessment or risk treatments may need to be revised.

Resolution

The wording of this principle requires revision to make the intent and desired outcome clearer. For example, changing the 'principle' to better reflect that risk management helps people to be more anticipative and better at detecting changing conditions.

[48] Although, admittedly, risk management when controlled by AI, may in the future actually become anticipative.
[49] Not to be confused with the hijacking of the term by some consultancies, in order to rebrand fairly basic risk management methods.

vi) Principle: Best available information

It may be pedantic, but 'information' is different to 'data', and is different again to 'knowledge'. Risk management involves the use of all three, as well as the next conceptual extension of 'wisdom'. Whilst the terms may at times be used synonymously by the general public, the terms carry very different specific meanings in decision science and other related disciplines (Sanders, 2016; Sing et al 2010), differences that should be acknowledge by the Standard.

There are a number of attributes associated with this principle that are vague or ambiguous, and are open to multiple different interpretations. This principle, like many of the others, provides insufficient information for effective guidance. The reader is left to assume that 'best available', only means information that is "timely, clear, and available". Surely there is more to the concept of "best available"? Even these individual attributes identified by the Standard requires further explanation.

What does "timely" mean? Does this require that the information is available (or becomes available) at the specific point in time when it is required by the risk assessment process? In which case what about vital information that may only become available later, could there be justification for delaying the assessment to collect the vital information? Or does 'timely' refer to the currency of the information, that it reflects the changing context? Or does it reflect an alignment with the different activities of the risk management process?

What about the attribute "clear", does this mean in a data format that can be analysed with the available tools and techniques? Data and information that has been 'cleansed' and 'normalised' in a format that can be understood by the analyst? That the products of risk assessment are not vague or ambiguous for the end-user? Or that the format and language of the product cannot be easily misunderstood or misinterpreted, or be unacceptable?

Regarding "availability", does this mean only information that is routinely available, or only available by existing mechanisms? How does this relate to the need to introduce approaches for accessing so called 'dark data' which the analyst may not even know exists, let alone have the existing means to access (Hand, 2020).

This principle only provides a partial clue about what "best available information" may actually comprise. In its attributes of "best available information" it omits a range of equally, if not more important attributes and concepts, for example:

- Integrity and validation.
- Data cleansing and normalisation.
- Longevity.
- Accessibility.
- Accuracy.
- Precision.
- Reliability.
- Completeness.
- Relevance.
- Uniqueness.
- Consistency.
- Cost-benefit valuation[50].
- Conformity.

[50] Sometimes it may just cost too much to gather and use the best available information.

- Error.
- Compliance obligations.
- Confidence levels.
- Confidentiality and privacy

There will also be tensions in trying to achieve "best available information". How should these tensions be evaluated and managed, for example the potential conflict between completeness and accessibility, comprehensiveness and cost, etc.

We are in full agreement with this principle's statement that "Risk management explicitly takes into account any limitations and uncertainties….". However, anecdotal evidence suggests that this aspect of the principle is frequently ignored by majority of risk practitioners. For example:

- The large number of organisations that continue to use highly subjective qualitative assessments when there is readily available data on which to base a quantitative assessment.
- The number of organisations that use risk criteria that are uncalibrated and unvalidated, and where the analysts and decision-maker are unaware of the underlying assumptions that underpin these criteria.
- The widespread use of unvalidated risk matrices and heat maps.
- Perhaps of even more serious concern are those organisations and practitioners that persist in multiplying out ordinal scales[51,52] (e.g., substituting the descriptive criteria for the numbers 1 to 5 on the axes of a risk matrix) to provide a mathematically unsound pseudo quantitative analysis.

By being also largely silent about the benefits of sensitivity analysis, uncertainty calibration, and confidence estimates, and by equally promoting both qualitative and quantitative analyses, the body of the Standard is certainly not advocating for adoption of the principle of 'best available information', or being consistent in guiding practice.

Resolution

The Standard needs to provide more meaningful guidance on what constitutes "best available information" and how information quality assurance could be addressed.

[51] An ordinal scale is a scale that does not have a zero point, and does not provide a measure of the difference between the variables, giving just their relative ranking. As opposed to interval scales which provide equal differences between values, and ratio scales which provide a zero point and equal differences between the values which may include logarithmic differences to allow exponential values to be used.

[52] Commonly using an arithmetic progression to try to measure something that is exponential in character, another mathematically unsound approach.

vii) Human and cultural factors

The principle is correct in stating that "human behaviour" and "culture" influence risk management. However, unlike several of the preceding principles, this one is left as a high level generic statement, with no explanation of the rationale and importance of this.

"Human behaviour" and "culture" are mentioned several times[53] in the body of the Standard. On each occasion, the mention comprises an anodyne motherhood statement, with the reader being left to fill in the conceptual gaps with individual interpretations and assumptions (hardly meets the previous principle elements of clarity, comprehensiveness, or best available information, or is this a case of 'practise what we say, not what we do?).

Surely something that is so important that it warrants its own 'principle', in the Standard deserves more consideration than a handful of bland and vague statements[54], and warrants at least defining these terms (as relying on the OED[55] definition is wholly inadequate) in this situation.

One of the most informative and useful explanations of culture is that developed US academic Ed Schein[56], who described culture as comprising:

- The artefacts, those elements of culture that are most easily seen and experienced, this includes people's behaviours, documentation (like policies, and mission statements), organisational structures, behavioural codes, workplace design, industrial relations, senior management statements of intent and support, resource allocation, organisational priorities, expressions of commitment, provision of resources, etc.
- Explicit values, those expressed and recognised values, beliefs, and attitudes. These elements can be relatively easily detected, and directly influence the formation of the artefacts.
- Deep underlying assumptions and beliefs, which are hidden from general view, and those holding these assumptions and beliefs may not even consciously be aware of their existence without purposeful introspection. These assumptions and beliefs influence the formation of the recognisable explicit values.

From a risk management perspective, culture is an important consideration because it will influence, enable, and constraint how a risk management approach is designed, implemented, and sustained. It will influence how effectively and efficiently risks are managed, and how individuals and teams think about risk and make decisions about risk.

Since culture can have such a profound effect on how risk is managed, the design and operation of risk management arrangements is best undertaken considering how the prevailing cultures[57] will affect those arrangements, and affect how people perceive, make sense of, and make judgements about risk. It is important that the influences of 'cultures' are not only considered in the present, but

[53] "Culture" is mentioned six times, and "human behaviour" is mentioned only three times.
[54] Although we are thankful that the Standard does avoid using the awful confection of the 'risk culture' construct. Culture is an aspect of how people work together in groups. Processes and frameworks do not have a culture!
[55] Oxford English Dictionary.
[56] Schein, 1983.
[57] Yes, we use 'cultures' plural quite deliberately. Within any organisation there will most probably be multiple cultures, every different grouping of people (formal organisational structural units, leadership teams, ad hoc project teams, social and friendship groupings, etc.) will each have their own unique culture. Organisational culture is a reflection of how certain elements come to predominate and influence the organisation as a whole.

how evolution of these cultures (and the emergence of new cultures) may affect how risk is managed into the future.

Just as culture influences the management of risk, the way in which risk is managed will have some influence on the evolution of the different cultures within an organisation.

On human behaviour

The inclusion of "human behaviour" as a separate distinct element from culture is interesting, as many cultural models include human behaviour as a core element. This does raise the question, is this specific distinction of "human behaviour" a redundancy within the Standard (given it is part of 'culture'), or is there a particular reason for separating out behaviour? Unfortunately, like other parts of ISO 31000, the reader is left to guess about the true intention and meaning.

Just how important is consideration of human behaviour to risk management. Well, it can be important, how we perceive risk influences our sensemaking and decision-making about risk, which will consciously or unconsciously influence our behaviours. In turn our behaviours will amplify, moderate, remove, or introduce the conditions within which we will perceive and manage risk. But what does all of this mean for how we undertake risk management?

Well, perhaps those responsible for writing this principle, did not fully think the concept through. There is a whole area of science that considers how people go about their activities, 'human factors' (Stanton et al, 2013; PSNET, 2019; Flouris and Yilmaz, 2010; Salas et al, 2010; Henriksen et al, 2008; Reason, 1995; Allnutt, 1987). The area of human factors includes consideration of behaviour, but places it within a much broader analytical framework. A reasonable definition of 'human factors' is: "*the ways in which the organisation, the job, and the individual interact to influence human reliability…*"[58]. Although the whole definition relates to hazardous events (in this context to offshore energy operations), the key elements of human factors apply to any time we are thinking about risk and risk management (Wolers Kluwer, 2022; Yilmaz, 2019; Xuecai and Deyong, 2018; Balfe and Leva, 2014; Noroozi et al, 2013; Stanton et al, 2013; Reason, 1995).

Resolution

It seems that the Standard is confused by the concepts. By "human behaviour" we think that what the Standard attempted to do (but did not have the language for) was really to highlight the importance of 'human factors' in risk management. Human factors analysis is not a common practice for 'risk professionals (outside of the safety disciplines), but is an area that can make almost immediate improvements to how risk is managed. This is not just about applying human factors to the assessment and treatment of specific risks, but how human factors can influence, enhance or limit how risk management arrangements are designed and applied. This is a high priority for consideration in the next revision of the Standard.

[58] NOPSEMA, 2021.

viii) Continual improvement

There is nothing majorly wrong with the sentiment of this principle, although it is rather weakly expressed. Yes, risk management can be improved by “learning” and “experience”, but these appear to be particularly passive approaches as written. Risk management will not be improved through ‘osmosis’, just because people are experiencing things. Even on those occasions when some passive individual learning is occurring, this does not mean that this learning will be shared adequately or that continual improvement will follow automatically.

The peer reviewed literature is overflowing with examples of where attempts at ‘lessons learned’ have failed to achieve any meaningful and sustained improvement (Proctor, 2020; Figueroa, 2016; Coles 2014 Schröder-Hinrichs, et al, 2012; Allington, 2012; Wright, 2010; Birkland, 2009; Allen, 2008; Donahue and Tuohy, 2006). Lessons learned needs to be undertaken as part of a planned and adequately resourced systematic and strategic approach. Similarly, individual and team experiences cannot be expected to drive improvement in risk management, unless these experiences are captured and used to gain ‘teachable moments’ and ‘actionable insights’ (Gibson and Gibson, 2023b; Morris, 2019; Gentry, 1990; Kolb, 1984)

Resolution:

‘Learning’ is referenced only once in the entire Standard (actually in this ‘continual improvement’ principle), which is surprising given that this should form the cornerstone of the principle. The whole concept of learning as a key component of risk management warrants a more comprehensive consideration in the revision of ISO 31000.

The section on the 'Framework'

Issue: Figure 3 does not represent a 'Framework'

Mistaking a PDCA process for a framework

One of the major problems with this section has been highlighted earlier in this Whitepaper, that is that the "Framework Figure" does not represent an actual framework of any description. The most generous thing that we can say about Figure 3 is that it is a generic process for developing and implementing 'something'. This very same process diagram could be equally applied to putting in place a financial accounting system, making a rubber widget, or putting together a certification program for car windscreen cleaners waiting at traffic lights.

Is this even a good process for designing a Framework?

Well, the process is a slight alteration of the traditional Shewart-Deming cycle (also known as a PDCA cycle – Plan-Do-Check-Act) that dates back to the 1930's (Johnson, 2002). The cycle has seen sterling service over the last 90 years or so, and is rightly credited with facilitating a large range of improvement and quality initiatives. However, the world has changed dramatically since the interwar years. For decades through the Twentieth Century, organisations have been able to use essentially linear processes like the PDCA, and although drawn as an iterative cycle, it is essentially a set of progressive linear steps used to solve predominantly linear problems (where cause and effect is apparent and can be simply described).

However, today we all pretty much operate in highly complex environments where we have to solve highly complex problems, contexts in which the PDCA cycle can struggle (Kemenade, 2014.). This is why approaches such as the PDCA have evolved, either with new tools being deployed along with variants of the cycle, or into markedly enhanced methodologies, such as 'Agile' and more explorative approaches (Furlan et al, 2023; Henriques et al, 2017). Even though the basic PDCA cycle is still used widely across many different types of organisations, its poor application has been criticised (Taylor et al, 2014).

It has also been cogently argued that using the PDCA cycle (or its variants) for *building* a system (or framework) is a de facto misuse. The PDCA was developed to *improve* a system, not to *create* one (Laquana, 2021).

PDCA and management system standards

One of the major problems is that ISO as an organisation is completely inculcated with the management system standards (MSS) ideology. The commonest feature across a multitude of ISO Standards is some variant of the PDCA cycle which forms the core of the MSS philosophy. Unfortunately, there is little robust causal evidence that the MSS approach results in any significant enhancement in performance in the areas covered by these diverse Standards. The majority of published research into MSS shows some *correlation* but little evidence for *causation*, i.e., there is a lack of evidence that MSS directly add value to the activities they are changing, just that improved performance sometimes coincides with an MSS implementation. That correlation is of course understandable, if an organisation is taking the time to implement and maintain a MSS, they are more than likely to be also undertaking a range of other improvements in their processes that will affect their performance. Something that most of the sparse research indicating some MSS benefits have largely ignored.

A few organisations have reported that such ISO MSS can provide 'internal benefits' such as "improved control and discipline" (Rayner and Porter, 1991), notably *not* enhancing performance. Whilst even those studies that show some positive *correlation* between MSS and performance, also report considerable problems with implementing MSS (Magd and Nabulsi, 2012).

Does the MSS approach really provide much benefit? The answer is 'yes', 'sometimes', 'maybe', 'probably not' (Bajec et al, 2013; Poksinska, 2010; Feng et al, 2007; Larsen and Häversjö, 2001; Seddon 1997a, 1997b). The best known and probably most widely implemented of the MSS is the ISO 9000 series of Standards. Although there are decades of experience in their use and years of research being conducted there is scant evidence that this MSS approach improves quality and performance[59] compared to almost any other alternative reputable methodology. Admittedly, some quality benefits have been reported (and again these may be more correlation than causation) following implementation of these MSS. However, those few situations where quality improvements have been reported are most commonly found in highly controlled and predictable component manufacturing processes. The sparse evidence in support of MSS (specifically ISO 9000 series) shows that improved performance can occur, but only "*in the complete absence of any alternative quality management approach"* (Gotzamani and Tsiotras, 2001; Buttle, 1997). In other words, if you are doing nothing at all to improve quality, then ISO 9000 standards may help, but probably not if you have any other quality management approaches in place. The mere existence of the ISO 9000 MSS has been called an "economic disease" and a "step backwards" (Seddon, 1997a).

To date, we have been unable to find compelling evidence for MSS causation in achieving elevated performance in highly complex and uncertain contexts. Over the last few decades there have been increasing questioning and criticism about the value of MSS and certification against these Standards (Zobel, 2018; Kafel and Simon, 2017; Zobel, 2015; Bernardo and Simon, 2014; Poksinska, 2010; Sampaio, et al, 2009; Casadesús, 2009; Dick et al, 2008; Franceschini, et al., 2008; Hertin et al, 2008; Casadesús and Karapetrovic, 2005b; Poksinska, 2003; Terziovski et al, 2003; Rondinelli et al, 2000; Goodchild, 1998; Krut and Gleckman, 1998). Adoption of MSS has also been connected with an increase in "failure risk" (Franceschini et al, 2018).

Where there are potential benefits for the adoption of an MSS, it is probable that these are achieved during the initial implementation of the Standards, with these initial benefits then declining over time (Casadesús and Karapetrovic, 2005a). The growing criticism of MSS has also been accompanied by a decline in both certification and use of MSS[60] (Franceschini, et al., 2010) in a growing number of geographic regions.

None of this is really surprising when one considers that the underlying purpose of the foundational MSS was to provide a compliance approach for the inputs, but not guarantee outcomes (Heras-Saizarbitoria et al, 2018).

Why this lengthy discussion about MSS? Two reasons:

- There have been 'pushes' from several directions to turn ISO 31000 into a MSS, rather than the current principle-based approach. This, despite the fact that there is far more evidence for the success of a principle-based approach compared to MSS (see above).
- The core engine of the MSS is the antiquated PDCA cycle, which since 2018 has also been the core engine of ISO 31000. Some Standards risk experts have remarked that this could be an attempt at MSS by stealth!

[59] The very purpose of the ISO 9000 series.
[60] Especially in the case of ISO 9000 series

Resolution

Whatever happens during the future revision of ISO 31000, the 'best bits' of the Standard must be retained, and that includes its principles-based approach.

A problem with linearity

Non-linear processes (for example, repeatedly reflecting and revisiting earlier activities as sensemaking and insight develop through the process) are required to solve the non-linear challenges of a modern world. Continuing to use outdated linear thinking and linear-based process (such as the PDCA) will be a retrograde step for the Standard.

One of the key fundamental problems of the original PDCA cycle (which the Standard's Figure 4 perpetuates) is that it continues to promote single loop learning, which is increasingly associated with poor learning and improvement. To deal with increasing complexity, the thinking has to transition (Lines, 2021; Tosey et al, 2012; McClory et al, 2017; Yuthas et al, 2004; Cartwright, 2002; Romme and van Witteloostijn) to double-loop, triple loop and quadruple loop learning (see Figure 4), if accelerated learning and innovation is to occur.

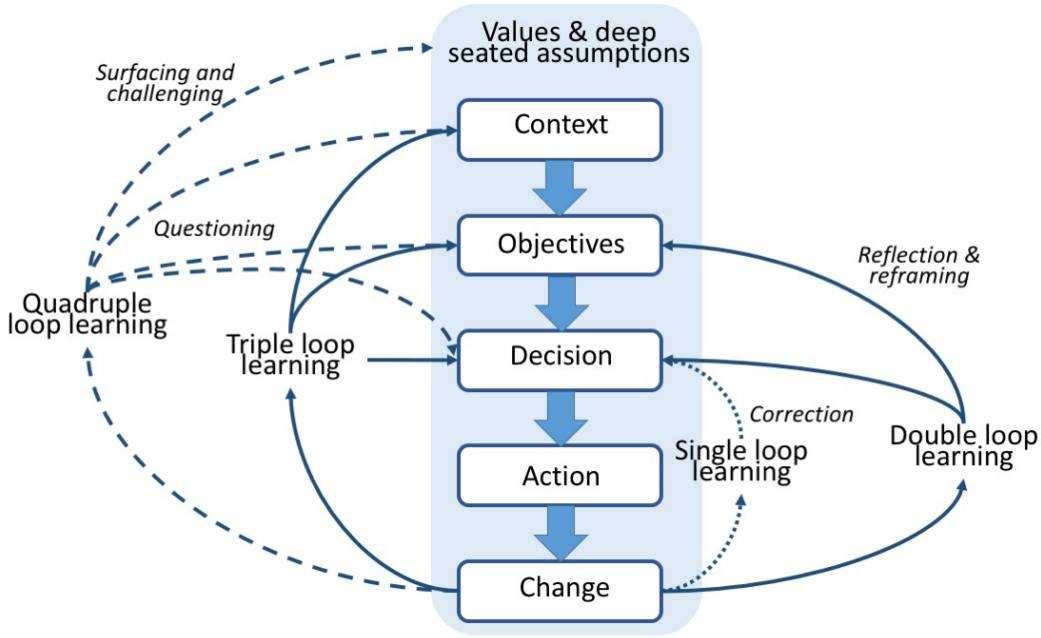


Figure 4: Organisational learning loops (reproduced from Gibson, 2020, with permission)

The PDCA addition by ISO 31000

The 'Framework' cycle in the Standard does have one addition to the traditional PDCA cycle, the inclusion of an extra step of "integration", placed towards the 'end' of the cycle. Since this activity is about 'integrating' risk management into the organisation, it is very puzzling why this activity occurs after the risk management framework has been designed, implemented, evaluated and then revised and improved. This really does not follow a logical flow.

Integration should start in the design 'stage', where understanding the need and limitations should form part of the problem definition that the risk management framework aims to resolve. The design of the framework should then take account of how this integration should be undertaken and should provide a plan by which the subsequent implementation will take place (which will drive that integration). It is during implementation of the risk management framework that actual integration[61] is enabled and facilitated. Similarly, the success of that integration forms part of the evaluation of the framework, which in turn informs the 'why', 'what' and 'how' for improving the framework, including strengthening and broadening the integration.

Why then does Figure 3 in the Standard have "integration" sticking out like a sore thumb after all of these other activities have been *completed*. This looks like a major logical error in the process flow.

The other major problem with Figure 3 (and is common to the PDCA cycle as well) is that the diagram conveys a cycle as a de facto perpetual motion machine. There is no indication of how this cycle commences and then sustains itself, or if the cycle pauses, or if it continues to the end of time. For example, where is the decision point on whether the cycle (and the framework) is still required, or needs to be decommissioned. Continual improvement does not mean continuing to run the same cycle over, and over, and over again

What does this all of this mean for the revision of ISO 31000:2018? Well firstly, the revision needs to recognise that 'integration' is not a standalone activity, 'integration' needs to be better integrated itself into the process, it needs to be an intrinsic activity that occurs across the entire process for establishing and sustaining a risk management framework. As discussed previously, the whole concept of 'integration' needs to be revisited and tested to see if it actually is an intended outcome, or if the concepts of 'embedded' and 'embodied' are more appropriate.

Secondly, the revision of the Standard needs to move away from concepts that have served for almost a hundred years, but are now becoming rapidly outdated. For many years, users of the PDCA (and its later variant the PDSA cycle) have recognised that just using the cycle as it is portrayed on its own is insufficient (Reed and Card, 2015), and that at a minimum it requires a more informative framework of analytics to support it[62], something that is certainty missing from Figure 3 in the Standard.

It should also be borne in mind that providing this PDCA cycle in the Standard could also be viewed as a prescriptive recommendation. Many organisations have in place effective contemporary design development, creative, and project management approaches (for example, such as 'Agile', 'lean', etc.), that would be in conflict with taking a retrograde step (by using the PDCA cycle) solely for building and improving a risk management framework.

Even just taking the old PDCA cycle[63] and adding in a review-reflect-revise cycle[64] would be an instant improvement. However, it must still be remembered that the PDCA cycle is a relic of early twentieth century thinking and business practices, where small incremental improvement was sufficient. For our current and future environment, incremental improvement is not enough, when Ministers, Boards, C-suites, customers, suppliers, employees, and other stakeholders are demanding innovation. Unfortunately, innovation is not within the DNA of the tired old PDCA cycle.

[61] However, see our earlier comments about the limitations of 'integration' thinking.
[62] Moen and Norman, 2009.
[63] Which even through the PDCA cycle is an aged veteran, it still makes more sense than the Standards' Figure 3.
[64] Which allows earlier activities to be revisited as more understanding and learning occurs through the cycle.

From the personal perspectives of the authors, in our practical experience the diagrammatic 'Framework" approach does not work as described, that is without substantial modifications being made. Even then there are far better ways of creating and managing a risk management framework.

Resolution

The revision of the Standard should consider abandoning the current 'framework' diagram and instead introduce a diagram that actually describes the concept of a risk management framework. Furthermore, including a PDCA cycle can be viewed as proscriptive, and the Standard should not be recommending a process that is becoming increasingly outdated.

Instead, the Standard should describe some of the key attributes for a process for creating and maintaining the framework, but remain agnostic with respect to the actual process. For example, this could include introducing Framework subsections on (but not limited to:

- Stakeholder needs analysis.
- Gap and requirements analysis.
- Human centric design approaches.
- Governance approaches.
- Structural elements.
- Performance evaluation.
- Sensemaking and decision-making.
- Treatment design and implementation.
- Risk intelligence and communication.
- Role of risk leadership.

Framework text

There is little in the body of the text under "Framework" that is actually about what could or should comprise a risk management framework. Almost all of the text in this section of the Standard is about explaining the components of the PDCA-like process diagram, not about an actual framework. The structure, composition, or operation of which is completely omitted from the Standard.

Issue: a lack of understanding about leadership?

We, the authors of this Whitepaper, would be amongst the first to shout out about the importance of "leadership and commitment" in risk management. However, section 5.2 of the Standard has little to do with leadership (and nothing to do with risk leadership), but everything to do with management and managerialism[65].

A too great a focus on managerialism has been frequently criticised for stifling innovation, freedom, creativity, agility, and adaptability, and removes decision-making from those with the best situational awareness and the ability to make the best decisions (Lumen, 2023; Klilkauer, 2013; Noveck, 2021; Lees et al, 2013; Alvesson and Sveningsson, 2011; Parker 2002). Managerialism is by its very nature detrimental to effective risk management, especially given the uncertainty, novelty, volatility, and turbulence that a majority of organisations now have to face. This form of managerialism is a relic of last century thinking, and should have little place in trying to address the volatility, complexity, novelty, and uncertainty faced by modern organisations.

Leaving 'risk leadership' aside for the moment, how relevant is this section of ISO 31000 to achieving an effective risk management framework? The Standard certainly places a substantial workload onto top management and oversight bodies (such as the Board). Whilst this wide range of additional accountabilities and responsibilities may feel intuitively 'right' to some, again the question must be asked if this is more well-meaning conjecture, with little evidence to back up the claims that have been made.

It is recognised that for many organizations, workload and stress have increased substantially over the last few decades, and that these trends are being accompanied by significant increases in both the risk and occurrence of burnout in both employees and 'top management' (Inegbedion et al, 2020; Lilly et al, 2019; Hussin et al, 2018; McCormack and Cotter, 2014; Halbesleben and Buckley, 2004). Yet ISO 31000 places even more workload on oversight bodies and top management, without evidence that this increases the effectiveness of risk management. Instead, the Standard recommends introducing an additional set of burdens that may distract these oversight bodies and top management from their primary purpose, which is to take and make decisions about risk.

[65] Managerialism is the reliance on (and the belief that it is necessary) on professional managers to undertake all planning and administrative functions.

What should oversight bodies and top management be focused on?
There is a case that can be made for certain statements to be retained or additionally included in this section of the Standard:

- Boards and top management are held *accountable* for managing risk in many jurisdictions. There may be legal obligations (legislation, regulations, and contracts), along with duties of care, codes of conduct, policies, etc., that specifically identify those obligations.
- Boards and top management are expected to actively *seek assurance* that risk is being managed effectively (this may even be a specific legal obligation, for example in some jurisdictions these are requirements in health and safety legislation, and companies and business laws).
- There is often an *accountability* for ensuring that the arrangements for managing risk are adequately resourced, that authority for making decisions about risk is delegated, and that responsibilities for the management of risk are assigned (however this may be almost impossible to specifically assign responsibilities for the myriad of risks that are managed on a daily basis.
- It is common for statements or policies to be created about the risk management approach. However, not all statements or policies are equal, there is no published evidence that shows how effective such pronouncements are (although there is evidence of poor performing risk management in organisations which have such policies and statements in place). We have to take it on faith that these artefacts are important, but the Standard provides no guidance (apart from the ever-common motherhood statement) about what attributes make an effective policy or statement.

Beyond these accountabilities, ISO 31000:2018 makes some assertions that cannot be justified. For example, that top management and oversight bodies have responsibilities for "customizing and implementing all components of the framework". This is frankly unworkable. Top management and oversight bodies should never have such a responsibility. They may make decisions that direct someone to establish a framework, and they may seek confirmation that the framework is actually working. However, they most certainly do not customise or implement any framework, that is the responsibility of people employed for that very purpose.

Similarly, section 5.2 of the Standard makes various claims that the few governance activities described within the Standard "*will"* help an organisation achieve a whole list of outcomes. Whilst these dot points seem intuitively OK, there is again no evidence supporting the effect of these "leadership and commitment" activities on achieving the outcomes. Without such evidence this is just speculation (especially problematic since the Standard states that they "***will*** help" (our emphasis). Looking at the ways in which organisations operate in the real world, it seems reasonable that these outcomes could still be achieved if the relevant activities were undertaken elsewhere and at lower levels of the hierarchy in the organisation[66]. So why place, what are essentially operational responsibilities, with the top governance and strategic levels of an organisation, in the absence of any consideration of cost-benefit?

[66] For example, it is not uncommon for top management to assign a specific budget for the running of a large business unit such as 'Legal, Governance and Assurance Services'. The middle manager in charge then decides how much to allocate to each of the different teams in his portfolio, including how much funding the Risk Manager receives to achieve the objectives set by that middle manager.

More confusion between governance and management

The remainder of section 5.2 appears to further confuse the distinction between the role of the governing body and that of senior ("top") management. For example:

- Ensuring that risk is managed when *setting* an organisation's objectives is not just a requirement for the oversight body. Whilst it is often the role of the oversight body to set the organisation's overall long term strategic direction (which may include 'top objectives'), it is management's responsibility[67] to then develop individual strategies and operational plans (with their own objectives). In doing so, it is accepted better practice for both the oversight body and management (at all levels) to consider risk in setting these objectives. In fact, one of the key reasons for 'integrating' risk management into the wider organisation is to include a consideration of risk into the strategic and operational processes conducted by management, a process where a majority of objectives will be established and validated.
- It is not just the oversight body's requirement to "*understand the risks … in pursuit of objectives*". This is also a core duty of all levels of management. It could even be argued that because the pursuit of objectives is a management activity, that the oversight body does not even need to consider risk in pursuing objectives, but rather consider the risk in *setting* objectives.
- Again "ensure that systems to manage such risks are implemented and operating effectively" is a management as well as an oversight body activity. It could also be argued that the oversight body seeks 'assurance' (assures) whilst management 'ensures' that what needs to be done gets done. This same argument can be extended to the other "ensure' dot points in this section.

This now brings us to the statement that we made earlier, that this whole section is about a very narrow and confused perspective on governance and management (and promoting managerialism), and has little to do with actual leadership. There is a substantial difference between governance and management (GGI, 2021; Communitynet, 2013), and between management and leadership (Arruda, 2016; Nayer, 2013; Toor and Afori, 2008; Borgelt and Falk, 2007; Kotterman, 2006). Leadership is about creating a compelling vision that people can follow, empowering people so that they can follow that vision, and is about facilitating innovation and success. Management is about administering the day-to-day 'stuff' (Gavin, 2019; Aruda, 2016). If the Standard includes mentions of "leadership", then it actually needs to include some meaningful content about leadership, especially 'leadership" within the context of risk management.

The term 'risk leadership' has been increasingly used in recent years (in a number of different contexts), however, there is no overall agreed definition of risk leadership, and the term can cover a number of concepts:

- Existing organisational leaders visibly embracing risk management, constantly showing how understanding risk improves their decision-making, and encouraging others to follow suit.
- Enabling cultures that support a broad and deep understanding of uncertainty and the effective management of risk (Majola, 2021; Gandz and Seijts, 2013).
- Setting a vision and direction for the future of risk management.
- Encouraging the application of the most effective and efficient strategies, tools, and techniques for managing risk (Wardman, 2020).
- Finding different approaches, beyond the confines of traditional Standards, to better manage risk in a complex world (Andersen and Young, 2020).

[67] And 'top' management's accountability.

- Inspiring teams to embrace managing risk as a core part of their purpose.
- Encouraging risk leadership at every level of the organisation, but especially close to where decisions are made that can most immediately affect the risk, for example, through 'deference to expertise' (Weick and Sutcliffe, 2015).
- Challenging the status quo and being recognised as a key knowledge broker (Holberton, et al, 2019).
- Being the facilitator and trusted insider, rather than an obstacle to 'risky' business operations.
- Establishing the management of risk as the core leadership skill of the organisation (McHugh, 2021).
- Understanding ways in which active leadership can promote risk management, whilst dysfunctional leadership (Roter, 2107) causes harm.

Resolution

Although the term 'risk leadership' may be regarded by some as another confection, ISO 31000 should at least consider some of its attributes and activities, even if the specific term 'risk leadership' is not to be used. The Standard also needs to clearly articulate the role of more general 'leadership' in establishing the value of risk management, and promoting its use strategically and operationally.

This section of the standard should also provide less confusing and more up to date guidance on the differences between governance and management within a risk management context.

There also needs to a more informed consideration of the role and duties of 'top management' with respect to risk management. It is a common default position within many ISO Standards to impose onerous responsibilities onto top management, with little to no evidence that this is effective or even an acceptable practice. This seems to be based upon hierarchical concepts more connected with 20th century thinking that with what needs to work in a more modern organisation. There is a wealth of peer reviewed published studies and real world examples (Dwyer et al, 2023; Howe et al, 2023; Rotteau et al, 2021; Cantu et al, 2020; Malish and Sargent, 2019; Veazie et al, 2019; Godlock et al, 2019; Weick and Sutcliffe, 2015; 2007; Chassin and Loeb, 2013; Christianson et al, 2011) that show increased performance and reliability can be achieved by delegating decision-making and action away from senior levels down to those lower levels with the best situational awareness and capabilities to undertake them[68].

Issue does the Standard know what "integration" means?

The explanation of "integration" as part of the "Framework", like many other parts of ISO 31000, comprises vague high level truisms, and does not really either explain what "integration" looks like or how this can be achieved. As raised previously, there is a difference between being "integrated' and being "integral". Is "integrated" the correct term to be used throughout the Standard, or should concepts such 'integral' (vital or critical), embedded, and embodied, be used instead?

The Standard also recommends that its particular single methodology is "integrated' into all aspects of the organisation, which would not constitute good practice. Ignoring the fact that some organisations will need to modify ISO 31000's approach (in some cases almost beyond recognition) for it to work effectively, there are also a whole range of specialist functions where a completely

[68] In high reliability organising this is known as deference to expertise.

different methodology may be required (such as treasury risk management, engineering risk management, economic modelling of risk, etc.).

Whilst “integrating” the management of risk into multiple areas and functions of an organisation may provide benefits, this does not mean that “integrating” the ISO 31000 way of risk management is the same thing.

The section on design

Section 5.4 of ISO 31000:2018 covers the subject of design (of the framework). This section appears to be a hotchpotch of different ideas, most of which are only loosely connected with "design". Whilst important aspects of "design" have been ignored.

One of the glaring omissions is the complete absence of anything resembling a design process. All but one of the subsections appears to be more associated with the eventual outcomes of design, rather than the actual design of a framework.

Resolution

The Standard should describe what effective design entails:

- Developing a full understanding of the problem space. Section 5.4.1 of the Standard describes in detail various different considerations about understanding the organization and its context. However, the Standard then fails to provide any guidance on how this information is used to define the problem space, to engage in foresighting to determine the needs for the framework, or to establish the objectives that will set the parameters for and inform the actual design. It is also important to not just look at the internal and external contexts, but also to understand how these contexts may intersect and interact to form the problem space that requires a framework approach to resolve.
- Establishing a planned approach for undertaking the design. For example, sections 5.4.3 and 5.4.4 discuss roles, responsibilities, resourcing etc., for *risk management* in general but not those elements required for the design of the framework.
- Utilising human centric design, to ensure that human factors and user needs are put at the centre of the design process (VicGov, 2022a; Landry, 2020). Elsewhere in the Standard, there is a great deal of emphasis on the need to consider human behaviour and culture generally in risk management, but consideration of these human factors is missing from the "design" section.
- Evaluating and testing the design throughout the design process to ensure that the design remains fit-for-purpose, particularly if the problem space shifts during the design process.

Issue: is there more to risk management commitment?

Section 5.4.2 of the Standard raises a number of questions that need to be resolved regarding "articulating risk management commitment":

- Is just "articulation of commitment" enough? Merely "articulating commitment" could be perceived as the way of many other top management pronouncements as "do as I say, not as I do".
- Surely it is as important (if not more so) to actually *build and demonstrate* commitment, rather than just speaking about it. In this respect it is important to establish why such commitment is important and what value it brings. The Standard also needs to provide guidance on what this 'commitment' looks like and what sort of actions and artefacts go towards building and demonstrating commitment.
- Whilst there is nothing wrong, per se, with the dot point list in this section of the Standard, it does omit some critically important things that top management and oversight bodies should be doing.

If they are actually committed to risk management, rather than just trying to look as they are, they should demonstrably always be thinking about uncertainty and risk in their deliberations and decision-making. It would be a reasonable assumption that most 'risk professionals' are aware of senior people in organisations that *speak* about the need for each of the elements in the list of dot points in this section of the Standard and periodically accept risk reports, but then do not use this information in their decision-making.

- If this "commitment" aspect of the framework is actually working, then how can it be shown that it is making a positive difference to how risk is being managed, and how could this difference be measured?

Issue: how can we know who owns risk, before we know what risk is?

Section 5.4.3 of ISO 31000:2018 concerns assigning "authorities, responsibilities, and accountabilities…" for risk management. This is an incredibly important aspect of risk management, but again is dealt with superficially within the Standard. The Standard appears to be confused about the difference between the design of the 'risk management framework' and the design of the 'risk management process'. It can be debated as to the extent to which an oversight body's role is to "assure" that activities are undertaken, or whether it is to "ensure" that the action occurs. The latter implies a far more interventionist involvement than would normally be the case for an oversight body.

This confusion is reflected in the preceding section's list (section 5.4.2 of the Standard) which includes several responsibilities that should rather be exercised by persons other than the oversight body and top management.

Section 5.3.4 also states that "risk owners" be identified, presumably during design of the framework (since it is in the "design" section). This seems to be an inappropriate activity during design as it is before there is any identification of the risks that will need to be managed and owned. Whilst it may be possible to assign "risk owners" at a risk category level (if a categorisation scheme is used) this also seems premature during *framework design*, where it would seem more appropriate to identify and involve relevant *stakeholders*.

Resolution

The concept of risk ownership needs to be better explained in the Standard, especially how it is assigned and when it is assigned.

Issue: communication and consultation the managerialism way!

Section 5.4.5 of the Standard covers communication and consultation, apparently with respect to "design". However, the text in this section is not 'design specific,' providing only a very general consideration of these two activities. Communication and consultation as described does not relate specifically to the risk management framework, and is so generic that it could not only be applied to anything to do with managing risk, it could also be applied to almost any other function or activity of an organisation.

Furthermore, the content of this Section is superficial (providing no real guidance in relation to the risk management framework) and fails to recognise the significant evolution that has occurred in communication and consultation over the last three decades. There is much more to these two concepts than just "sharing information" with people and seeking 'feedback'. Effective communication and consultation are about being able to see the world from the different perspectives of different stakeholders. It is about understanding the information needs of these stakeholders, and the value of stakeholder contributions. It is about engaging with stakeholders, facilitating their participation, and understanding the factors that will enhance or constrain such engagement and participation. Above all else it is about understanding which stakeholders can provide value and how to incorporate that value into risk management (and in the case of this particular section, specifically about the contribution of communication and consultation to the framework).

Effective communication and consultation is not an *ad hoc* activity, it needs to be planned with clear objectives and a systematic process for achieving those objectives. This should include surfacing and challenging the assumptions that underpin both the approach and the outputs of communication and consultation. The approach described in Section 5.4.5 of the Standard is significantly below the generally accepted practice models. There is a real possibility that poorly planned attempts at communication and consultation become perceived by stakeholders as tokenism or prevarication, resulting in a more negative impact than if no communication attempt was made at all.

Resolution

There is a wealth of freely available published guidance that is relevant to this section of the Standard, a lot of which has years of experience and evidence to support its contentions and the effectiveness of it use[69] (SCV, 2022; VicGov, 2022b; UNEP, 2020; Gold Standard, 2019; Biodiversa, 2014; IFC, 2007; Krick et al, 2005; Zohar et al, 2005). The Standard needs to provide guidance on communication and consultation that is directly relevant to the risk management framework (and subsequently for the risk management process).

Despite some differences in some of these better practice approaches, there are consistent themes across many of them, that can be considered for inclusion in the Standard:

- Understanding that stakeholders have different needs, beliefs, assumptions, and biases, that they will seek different types of involvement with an organisation, will seek different types of information, and will contribute different types of information.
- Whilst seeking diversity and inclusivity can be important, it is also necessary to recognise that at different times, the involvement of some stakeholders will be a higher priority and more

[69] Many of these publications are about wider community or public engagement, however there are many good practices and lessons that are directly relevant for risk management.

valuable than others, and these priorities can change over time. This may require deliberately excluding some stakeholders from participating.

- The need to facilitate meaningful participation of stakeholders.
- That communication and consultation is not merely a simple exchange of information ("sharing information" and "feedback"), but that it may need to involve establishing a continuing dialogue as well as facilitating participation in decision-making. The latter can be particularly important in designing and implementing a risk management framework, as many of the identified stakeholders may be expected to use the framework or be in some way affected by the application of the framework. This means that the stakeholder composition for the design of the framework (managers and key staff that will be applying risk management) may be different from the stakeholders involved in the risk management process (e.g., risk owners, process owners, subject matter experts, etc.)
- Clarity, transparency, and accountability are a necessary part of communication and consultation. Stakeholders need to be able to understand and trust the process and the implemented framework, and the motives of the people managing it. Outside of the specialised world of the 'risk practitioner', the very idea of someone coming into parts of the organisation and talking about risk can be threatening[70]. The integrity of the process. the confidentiality of the information exchanges, and privacy considerations for those involved are also important considerations.
- Using a balanced approach: whilst it may be desirable to include a vast array of different stakeholders in communication and consultation, this desire needs to be balanced against the costs and time that this would take and the real value that each stakeholder will contribute. These considerations also need to consider the relative value of stakeholder involvement, and the ability to analyse and make use of the quantities of information acquired.
- The timing, degree, extent, depth, and intensity of communications and consultations: Engagement and consultation need to avoid being too shallow so that little of value is obtained, balanced with the potential to be overwhelmed by the number of interactions and volume of information exchanged.

Communication and consultation concerning risk also needs to take account of various psychological and personal issues, including:

- The truthfulness, integrity, and credibility of those involved.
- The effect of biases on how information is provided, how it is 'filtered', and how it is interpreted.
- The potential for triggering adverse emotional and psychological responses in those involved.
- The desire for self-interest and self-protection that will influence preferential selection of some information, and suppress other information (e.g., partial disclosure).

[70] For example, some managers and employees will perceive a 'risk manager' like they perceive an internal auditor, somebody poking around trying to find out things that are going wrong and expose them to the rest of the organisation.

The section on “Implementation”

Issue: will implementation work in this way?

Section 5.5 of the Standard describes “implementation” in fairly simplistic and superficial terms. The description provided is a very basic plan-based deployment approach, and is highly unlikely to be successful if tried as is. There is substantial body of published articles that describe just why such planning and implementation approaches regularly fail (just a small sample includes: Casey, 2019; Marle and Vidal, 2016; Walker et al, 2013; Matta and Asheknas, 2003; Rodrigues and Bowers, 1991; Clark, 1981).

Resolution

Implementing an effective risk management framework needs to be undertaken as a managed change project, and should include consideration of activities such as: conducting readiness assessments, exploring engagement approaches, using behavioural insights, building a behavioural promotion and resistance management plan, employing project management tools and techniques, and very importantly having capable leadership in place.

Issue: a superficial evaluation

Section 5.6 of the Standard covers evaluation[71] of the framework However, it does not provide even a basic consideration of what evaluation should look like. It is not surprising that many ‘practitioners’ might simply ignore this section, and consequently do not perform a systematic evaluation of their risk management framework and its performance. In a similar vein, it is also uncommon for any meaningful evaluation to be conducted of the effectiveness of the risk management process itself. It appears that the majority of evaluation attempts focus on the inputs[72] rather than the outcomes of risk management[73,74].

[71] The use of the same word for different activities has caused some confusion in other parts of the Standard. Evaluation of the risk management framework and the risk management process is different to the evaluation ‘step’ in the risk management process. The former two are about the effectiveness of capability for risk management, the latter is about providing parameters for making decisions about risk.

[72] Resources allocated to risk management, presence of a framework and risk management process, use of risk assessments across the organisation, regularity of reporting to senior leadership and governance bodies, etc.

[73] Cost/benefit of the end to end risk management, quantitative value of the efforts to reduce uncertainty, improvement in the performance of decision-making, direct contribution to indicators of organisational success, satisfaction of decision-makers with the value provided by risk management etc.

[74] For example, there are multiple jurisdictions that undertake some of form evaluation of ‘risk management’ across government entities. These often take the form of evaluation questionnaires (commonly self-administered) where conformance with the relevant risk management standard (ISO, national, or government specific) is scored on Likert scales, or through other forms of maturity estimation. These evaluations usually provide a ’measurement’ of the presence of inputs, but provide little meaningful insight as to whether the approach is appropriate to individual contexts, that good decision-making is occurring, or that risk is being managed effectively. Having seen the outputs of several of these evaluations of organisations that have achieved high ‘evaluation scores’ for risk management, their actual performance in the real world was one of significant failures in public policy, frequent emerging and recurring crises, poor decision-making, and toxic cultures.

Evaluation is a vital activity, because without it the "framework' could be worthless, or even be causing real harm to the organisation. There are a number of evaluation philosophies and methodologies that are readily available and provide insight into how different evaluation needs may be approached (McGill et al, 2020; Jafari et al, 2011; Bayer, 2007; Saunders et al, 2005; OECD 2019; Tukel and Rom, 2001; Mark et al, 1999; Rohrmann, 1992). There are different types of evaluation that need to be considered:

- Structural evaluation: concerns the continuing presence, quality, integrity, availability, and the extent of use or uptake of the framework and its constituent parts.
- Process evaluation: concerns the effectiveness and efficiency of the implementation of the framework, and of associated improvement processes.
- Impact evaluation: the extent to which the framework has achieved its objectives.
- Outcome evaluation: the extent to which the overall goals for managing risk have been achieved and the nature of the contribution of the framework to achieving the organisation's strategic and operational objectives.

The development of any evaluation criteria needs to be informed by understanding the decisions that will be informed by these criteria, and by key principles that guide their design and operation. Those evaluation criteria that do not inform a decision, really provide no useful purpose. Decisions may need to consider, for example:

- The extent to which aspects of risk management are meeting expectations and need to continue.
- Those aspects where further investment and improvement are required.
- Where risk management needs to change its focus.
- Whether obligations have been met.
- The extent to which the framework (also process, program, etc.) has contributed to reducing uncertainty and the value this has provided to enhanced decision-making.
- How organisational learning has improved, and how further improvement can be facilitated
- The extent to which accountability has improved, and to which broader governance has been strengthened

A baseline suite of evaluation criteria (OECD, 2019) may be built on the concepts of:

- *Relevance:* the extent to which the evaluated elements meet or contribute to the objectives for the risk management framework and process, and for the organisation.
- *Coherence:* the alignment and compatibility of the risk management framework and process with other systems, frameworks, and processes. This coherence may be 'internal (looking within the organisation) or external (looking at the alignment and coherence with other organisations, such as industry partners, customers, supply networks, other critical interdependencies, etc.,
- *Effectiveness:* the extent to which the various aspects of risk achieve their intended outputs and outcomes.
- *Efficiency:* The extent to which the risk management framework and process achieve their objectives with budget and time requirements.
- *Impact:* The objective differences and their significance, that the use of the risk management framework and process makes.
- *Sustainability:* The extent to which the benefits, realised from the application of the risk management framework and process, will endure.

Evaluation requires careful planning and requires an understanding of what evaluation is trying to achieve (evaluation objectives). Evaluation requires a framework within which it will be conducted, for example a systematic evaluation process and criteria against which the evaluation will be conducted.

There are also other criteria with the current Standard, such as the (often ignored) 'principles' (section 4 of the Standard), that not only provide a suite of criteria for guiding design, but can also provide a foundation for the evaluation criteria.

The section on improvement

Issue: does the Standard understand adaptation?

Section 5.7.1 of ISO 31000:2018 provides a single sentence about monitoring and adapting the risk management framework, and in doing so misses out some important considerations, including:

- What is the purpose of this monitoring and adapting? Does it relate to just the risk management framework (given that it is in the framework section), or does it also include the risk management process as well. Is its purpose to monitor:
    - the continuing relevance of the objectives applied to the framework?
    - that the framework is being applied as required?
    - the performance of the framework in achieving its objectives?
    - the efficient utilisation of resources applied to the framework?
    - stakeholder understanding about the framework?
    - stakeholder acceptance of the framework?
    - fitness for purpose of the framework in a changing context?
    - relative cost/benefit for the framework?
    - effect of any alterations made to the framework post implementation?
    - The changing nature of the context within which the framework operates?
- How monitoring objectives should be established.
- What elements should be monitored.
- How monitoring will be conducted, including considerations of the breadth, depth, and timing of monitoring activities.
- The tools and techniques that will be adopted for monitoring.
- How issues such as early warning indicators, signal recognition, and noise will be addressed.

It should also be noted that 'adaptation' does not automatically follow 'monitoring'. There are a number of other activities that will also need to occur: information from monitoring must be collected, collated and analysed. The analysis must then be interpreted (made sense of), decisions made, and actions taken before any 'adaptation' can occur.

This section is also potentially confused with respect to specific terms that have been used. There is a material difference between 'adjusting' and 'adapting' something. Adjustments are often defined as small corrections or changes, as opposed to much larger transformations (adaptations). Another key difference is that adjustments are often made as a result of detected issues or in *anticipation* of future change occurring, whereas adaptation tends to occur in *response* to changes and the effect of stressors on the system.

Resolution

The revision of the Standard should consider including guidance on establishing an effective approach to monitoring, and how monitoring can be used to facilitate and drive change and improvement. The revision should also include guidance on different aspects of improvement and change, including a more detailed discussion of concepts such as adjustment, adaptation, transformation, managed change, etc.

Issue: should improvement be more than just incremental?

Section 5.7.2 of the Standard ("continually improving") is very brief (just three sentences) and generic, especially for something so central to and important for sustaining an effective risk management framework. The described approach also seems to be very passive and incremental, i.e., find something wrong or ineffective and produce a specific fix. Continual improvement is not just about undertaking such incremental improvements, especially where a sole focus on incrementalism can actually hinder future adaptation. Contemporary approaches have a dual focus on incremental continual improvement combined with 'future oriented breakthrough innovation' (Sebas, 2023; Klein, 2022; Lewis, 2022; Coleman, 2020; Schroedel, 2019; Madrigal, 2011). The question should also be asked if improvement should just be *continual* or if it should also be *continuous*.

Resolution

For the risk management framework, applying this section of the Standard should consider not just 'improving' how the framework works, but also transforming the whole way that the framework is structured, operates and performs. Such an approach can be greatly enhanced by undertaking improvement, reengineering, and transformation as part of as systematic approach to establishing a 'learning organisation' (IHI Team, 2021; Messnarz et al, 2006).

The section on "Process"

Section 6 of ISO 31000:2018 describes a risk management process that is centred on Figure 4 of the Standard. This is a modified version of the original process developed by Australian Standards (AS/NZS 4360: 2004).

Unfortunately. in the desire to have something looking more "21st Century[75]" by placing the process inside an arrowed circle, much of the nuance of the original process has been lost. Figure 4 is a poor directionless representation of the process, and does not reflect how effective risk management is undertaken in practice. The continually recursive and reflexive nature of the original process has been lost. Whilst the nature of the flows of activity, information, and understanding that the diagram should make clear, are instead confused and flawed.

Some activities, such as "Communication and Consultation" and "Monitoring and Review" 'float around' disconnected, and appear to have some vague one directional relationship with the 'risk assessment box. Instead of what should be intimate two-way interactions occurring throughout all of the activities. Similarly, the "context" and "risk treatment" boxes are left disconnected from everything else that is occurring during the process.

The inclusion of a "recording and reporting" element at the bottom of the diagram seems to be misplaced and occurring as a final afterthought, and appears to feed (in one direction only) into risk treatment, rather than receiving information and providing it to the rest of the risk management process. The accompanying text in the Standard does little to improve on the clarity of the risk management process. It should also be noted that in the original AS NZS 4360 Standard recording and reporting were fundamental elements of the "monitoring and review" activity. It is uncertain what benefit has been achieved by now creating 'recording and reporting as a completely separate activity in ISO 31000[76]. One would normally expect that recording and reporting would be a fundamental component of 'monitoring and review', which in turn occurs as a core activity within all parts of the framework and risk management process. This also raises another important issue ignored by the Standard, and that is that these overarching terms (monitoring, reviewing, recording, and reporting) may be very different activities with different purposes, approaches and outcomes, in different parts of the framework and process.

Figure 4 in the current Standard is a retrograde step from the previous process diagram used in the 2009 version of the Standard, and adds to the confusion and misunderstanding of many of its users, and has more resemblance to geometric art than it does to a logical process diagram.

Stepping away from the manifest problematic design of the Standards' Figure 4, the actual risk management process it is trying to describe, is in itself significantly flawed. This risk management process does not represent good practice. Despite being 'circular' it is still in essence a highly linear process, this linearity being further reinforced by the use of such terms "steps" and "stages" when referring to the process in different parts of the Standard. Such a linear approach to risk management can be effective in relatively simple contexts characterised by linear cause-and-effect relationships (such as mechanistic systems and situations). However, such approaches can struggle in more complex socio-technical systems (Gibson and Gibson 2023a) as relationships become increasingly non-linear.

[75] A personal remark made by one of those involved in the development of the diagram, which in the desire to look modern has instead created a vague process that seems to have some unclear circular activity occurring outside of it.

[76] Which seem to be the antithesis of 'integration'!

A more effective method for risk management is to use a more flexible non-linear approach, where the process does not follow separate steps but is reflective, recursive, and reflexive (Figure 5), an approach adopted by recent Australian Standards publications (Australian Standards, 2023a, 2023b). This process is better aligned with risk management and decision-making work in the real world:

- The presence of uncertainty and ambiguity throughout the risk management process (but especially in earlier activities) necessitate the regular surfacing and testing of assumptions and revisiting understanding gained earlier in the process. Information will always be imperfect in risk management, so judgement must be exercised in determining when and how often earlier activities should be revisited. This will usually be dependent upon the balance between the 'benefit' of additional insight traded off against the 'costs' of reducing data and information uncertainty.
- Whilst the context is being established, we are already beginning to get an insight into the nature of risk, we are beginning to identify risks and may even be undertaking some initial 'intuitive' analysis.
- As we progress, less time is spent considering the context and we have an increasing focus on identifying risk, during which time we may also be commencing some more involved analysis.
- As we uncover more insight into the nature of risk during analysis, we may have to keep going back and uncovering more information about the context or modifying our identified risks.
- Similarly, as the detailed analysis of risk proceeds, we are already gaining some insight into the importance of risk (the start of evaluation), but may still need to revisit earlier activities, to gain more information or to modify previous assumptions.
- As evaluation progresses, we may again need to revisit earlier assumptions. Whilst making decisions about the need to address these risks, at the same time we are beginning to develop insights into treatment, and so on through the rest of the process.

The idea behind this organic risk management process is that we do not naturally tackle risk as a rigid linear set of sequential steps (for example, consider how we manage risk in our daily personal lives, or when we need to make decisions in rapidly changing situations), but have a much more organic free-flow of exploration. This mirrors how decision-making occurs, an organic process, rather than a simplistic linear set of steps (Klein, 2008; Klein et al, 1993).

Whilst this organic risk process can be very effective even for simple linear contexts, it comes into its own in dealing with high uncertainty and complex environments, and especially for trying to resolve risk associated with wicked problems (Head, 2014; McMillan and Overall, 2016; Palmer, 2011; Head and Alford, 2008).

The organic risk management process is very closely aligned to Daniel Kahneman's (Nobel Prize winner) work on the psychology of judgement and decision-making (Kahneman, 2011; Kahneman et al, 2000; Jacowitz and Kahneman, 1995; Kahneman and Tversky, 1979), the work on naturalistic decision making in complex settings, and decision-making under uncertainty (Klein, 2023; 2015; 2008; Kaplan et al, 2021; Isler et al, 2020; Rosqvist et al, 2017; McCarthy et al, 2016Cunliffe, 2016; Kockenderfer et al, 2015; Starcke and Brand, 2012; Polasky et al, 2011; Trimmer et al, 2011; Fischer et al, 2010; Schultz, 2010; Platt and Heuttel, 2008; Bertsimas and Thiele, 2006; Bond and Cooper, 2006Gladwell, 2005; Tuddenham, 2000).

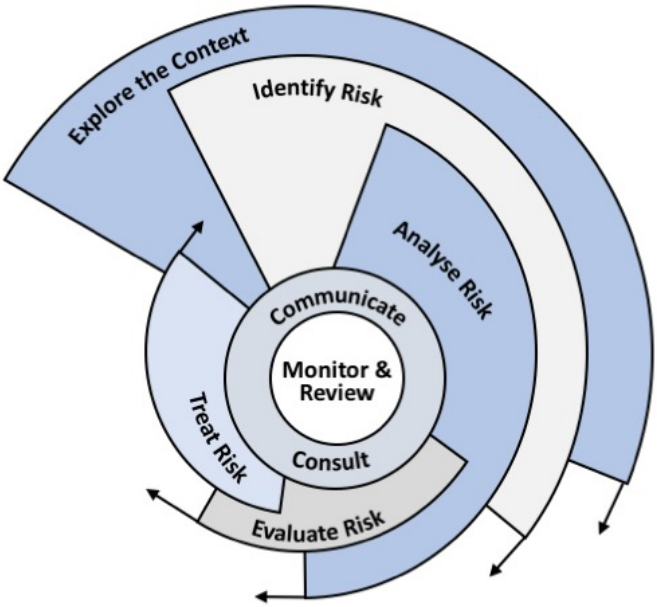


Figure 5: Organic risk management process[77]

Issue: what is section 6.1 "General" trying to say?

We have previously discussed, in this Whitepaper, the distinctions between the concepts of 'integrated', 'integral', 'embedded' and 'embodied'. This "General" section of the Standard tries for the first time to make a distinction. Yes, risk management is "an integral part of management". Risk management is an essential activity that is part of the way in which many organisational systems and processes should work. However, no, risk management should not only be "integrated" (as stated elsewhere in the Standard). By using the term "integrated", the Standard is stating that risk management process should just be linked to or coordinated with other activities, a bolt on process that is conducted alongside other functions. Thus, the term 'integrated' promotes a much looser relationship, than compared with the concepts of 'embedded' or 'embodied'.

The Standard also states "… can be many applications of the risk management process within an organisation, customized… context in which they are applied". This is an incredibly important concept, and one we fully agree with. However, we have found that this concept is widely ignored by many 'risk practitioners'. It is not uncommon to see the same methodology, tools, and techniques applied unthinkingly to widely different contexts, irrespective of any unique needs that may be present. For example, where a 'risk manager' has tried to force the corporate qualitative risk assessment process (as the enterprise-wide standard) onto technical specialists using bespoke quantitative modelling techniques developed specifically for their discipline. Similarly, on occasion, we have seen the identical risk criteria applied to the whole of enterprise level, to functional units, and to small projects, with such poor granularity that their use provides little insight for the local manager or project manager[78].

[77] Note "recording and reporting" which is separated out in the Standard, is not included in Figure 4 above, because these two activities are implicit within the other activities, with a major representation in the 'monitor and review activity.

[78] For example, a loss of $200,000 at a global corporate level may be insignificant, but within a local business unit or for a small project, this amount could be a major existential loss.

We have also seen internal auditors report adverse findings because of different customised risk assessment processes (that were validated) for being "non-compliant" with the unvalidated corporate process[79], or even worse, 'non-compliant' with the Standard itself.

ISO 31000:2018 also states in this "general" section that "human behaviour and culture" should be considered. To interpret this vague statement requires a lot of assumptions to be made about what is exactly meant by this. For example, does this mean human behaviours and culture:

- As a source of risk (hazard and threat)?
- As an influence on the sources of risk?
- As a vector through which hazards and threats could interact with the organisation?
- As control mechanisms that could modify the risk?
- As an influence on the participation of stakeholders?
- Having an effect on the presentation of information (e.g., selective pressures?).
- As an influence on the risk modellers and analysts, affecting the risk assessment?
- As an influence on decisions made about treatment options, or other aspects of risk?
- As an influence on sensemaking and decision-making informed by a risk assessment?
- As limiting or enhancing factors on the successful implementation of decisions?
- Affecting how monitoring and improvement is undertaken?

Although we believe that all of these factors are important considerations, in practice we have seen many of them consistently ignored by many 'risk practitioners', perhaps because the Standard provides such vague guidance in this respect.

The final statement from this section of the Standard is "although the risk management process is often presented as sequential, in practice it is iterative". Logically this sentence makes little sense, 'sequential' and 'iterative' are not mutually exclusive. A process can have both attributes (and many processes are). This issue has arisen perhaps because 'sequential' and 'iterative' were not sufficiently understood in the writing of the Standard. "Sequential' means following a logical set of steps, and is exactly what Figure 4 in the Standard shows, and this is exactly the way that the body of the Standard describes risk assessment. Being sequential does not stop it from also being iterative. Iterative simply means that once the sequence of steps is completed, the process is repeated over and over again. Neither of these two concepts reflect what effective risk management really looks like.

Resolution

Most of the issues with this section of the Standard require clarification and a more expansive explanation of the assertions. This section of the Standard also needs to be more cognisant of the research and published literature about risk analysis science and about decision science, and to incorporate this thinking and associated practices into revision of ISO 31000:2018.

[79] This got to insane levels in the early application of risk management Standards. AS/NZS 4360: 1995 provided a risk matrix as an example, which was subsequently misunderstood by internal auditors, that raised non-compliances when an organisation used a matrix that did not exactly match that in the Standard. This misunderstanding was so prevalent amongst auditors and practitioners, that the matrix was removed to an informative appendix at the back of the 1999 Standard. Misunderstanding about 'compliance' with the Standard's matrix became so widespread, that the offending appendix was completely removed from the 2004 version of the Standard.

The Section on communication and consultation – section 6.2

This Whitepaper has already made extensive comments about communication and consultation with respect to the risk management framework, and most of these comments hold true for communication and consultation associated with the risk management process.

The first part of this section 6.2 of the Standard clearly states that the purpose of 'communication and consultation' is concerned with the outputs of the risk management process. This is misleading on a number of points. Firstly, the purpose of 'communication and consultation' is not just limited to the outputs of the risk management process. It is a critical activity throughout the risk management process. Secondly, communication and consultation that is concerned with risk management outputs" includes the highly technical field of 'risk communication' (Balog-Way et al, 2020; Lundgren and McMakin, 2018; Heath and O'Hair, 2010; Renn, 2008; Gutteling and Wiegman, 1996; Covello, et al, 1986), a combination of psychological and social sciences, an aspect that is completely ignored by the Standard.

It is widely accepted that a dialogue with stakeholders is essential to better understanding the context, obtaining data and information for the risk assessment, gaining insight into the acceptability of risk, for testing the reasonableness of the analytical approach, and for developing and evaluating treatment options. Although this more expansive perspective is alluded to later in the section, having such a misleading statement at the start of the 'communication' section in the Standard has already primed the readers' misbeliefs before they read anything else. The Standard also demonstrates a very incomplete understanding of the nature and purpose of consultation.

The dot points that describe the aims of communication and consultation are somewhat vague and not entirely accurate:

- The Standards states: "Bring different areas of expertise together for each step..." We do not necessarily want to bring expertise (or experts), from different areas together for *each* "step". We want to keep important and necessary stakeholders informed about the process, and where necessary participating in and contributing to the process. We want to source information and we want to have access to relevant expert knowledge to provide input into the assessment of risk and the development of treatment options, and to help test our assumptions. But only in those *parts of the process where this will add value*.
- The second dot point is highly restrictive, different views are not only considered when defining risk criteria and when evaluating risks. Effective risk management should also be seeking appropriate views during assessment, treatment, during monitoring and improvement. Such views should also be sought to ensure the communication and consultation activities are actually meeting the organisation's and stakeholders' needs.
- The third dot point in this part of the Standard refers to "risk oversight". This is a fairly vague confected term, does the use of this term mean "oversight" of:
    - individual assessed risks?
    - risk communication?
    - the risk management methodology (e.g., that documented procedures are fit for purpose)?
    - the deployment of the risk management process and its accessibility?
    - the conduct of individual applications of the risk management process (e.g., for the corporate risk assessment, for project x, project y, for the compliance framework, etc.)?
    - is the term an alternative for risk governance?

It should also be noted that communication and consultation are only one of the sources of information that are necessary for 'oversight'.

Resolution

This section of the Standard requires review to establish the purpose and objectives of 'communication and consultation', as these are currently unclear, in what is superficial content in the Standard for such a major element of risk management. A more comprehensive suite of content should be developed to cover the various different aspects of communication and consultation that are essential for risk management to be effective.

The section scope, context and criteria

Section 6.3.1 starts off a little confused, the "purpose of establishing the scope, context, and criteria' is not to "customize the risk management process". The purpose of a scope is usually to define the nature of the problem that requires risk management, what is to be assessed, when it is to be assessed, and how it is to be assessed, and broadly how risk will be evaluated, how decisions will be made, and how treatment will be undertaken. This may also include an initial selection of the risk assessment methodology to be used, and the range of tools and techniques that will be employed. This is often summarised in a set of objectives for the particular application of the risk management process. Importantly the scope establishes boundaries and limitations, to ensure that the risk management process remains focused on what is required of it.

An initial scope should help direct (and constrain) the exploration of the context, during which any additional insight gained may require the scope to be revisited and revised several times. Part of this revision of the scope may indicate that the chosen methodology is not optimal and may require the chosen risk management process to be modified (customised), or replaced, or additional tools and techniques to be employed.

Resolution

This section is inaccurate and needs to be revised to reflect the actual purpose of the scope, context and criteria.

Issue: does anybody define the scope without knowing why?

Section 6.3.2 of the Standard tells us something about the importance of "scope" and what we should consider in planning the 'approach', but does not tell us what the scope actually is, or what its specific purpose is. Also, the majority of this section is about planning, (rather than the scope which is something completely different[80]). Again, we are provided with dot points of things to consider, but no actual guidance on how to develop a sufficient scope. Even if this section was headed 'planning', it would be insufficient, failing to provide even a workable approach for planning risk management activities [81].

Understanding the problem space

The one major omission in this part of the Standard[82] is the complete absence of any consideration of the 'problem space' (i.e., clearly defining the problem that risk management is trying to resolve). In other words, if the risk management process is the solution, what is the problem? With the follow on question: is risk management (generally) and the specific chosen methodology the right approach to achieve the needed solution to the problem? In practice, if one starts off with the premise that this is going to be risk management activity, then it predisposes that only risk management will be used, even when other alternative approaches may be a more appropriate solution to the problem.

[80] Scope sets the intent (the what), planning establishes how the objectives will be achieved (the how).

[81] Planning should perhaps have its own section in the Standard, or be a specific separate subsection under section 6.3).

[82] In fact, guidance on understanding the problem or the problem space is a major omission of the Standard as a whole.

It can be argued that the Standard's heavy linear process orientation negates appropriate problem space ideation and complex problem solving. Especially given that 'scoping' and 'planning' (as described in the Standard) appear to be highly activity-focused rather than problem-focused. This naturally leads to the main outcome becoming a 'risk finding exercise' rather than obtaining an appropriate and effective solution to a problem.

By defining the problem space, we can start to understand what needs to be achieved, and start the process of scoping out the risk management approach to look for answers to address the problem. Once the problem space has been defined, the purpose of the risk management activity (and how this will be approached) can be better defined: For example, is the purpose to:

- Comply with a specific requirement to undertake risk management (for example: to fulfil an obligation that relates to risk in regulations, policies, contractual arrangements, Board directions, etc.).
- Use risk management to drive the organization's compliance.
- Provide assurance that adequate or effective risk management processes are in place (for example in annual attestations required for government agencies in some jurisdictions.
- Provide assurance that risk is being 'managed effectively'[83] (for example, through Board reporting, project governance reporting, or annual attestations as above).
- Produce a list of risks (risk register or risk report) as part regular management and Board reporting.
- Rank and prioritise risk in order to allocate resources to 'modify risk' (risk treatment) to within acceptable limits.
- To provide automatic 'proceed' and 'stop' points (e.g., approval gates for project management, investments, mergers and acquisitions etc.)
- To inform decision making about strategic, operational, or tactical issues and options.
- To maximise benefits and minimise harm in pursuing opportunities.
- To drive strategic success.

Resolution

Section 6.3.2 of the Standard needs to consider how the 'problem' is defined for each particular application of the risk management process, to enable a better determination of the scope.

[83] Although most of these attestations seem to be based on confirming the presence of risk management processes (rather than success in actually managing risk), and rarely use robust objective measurable criteria. Risk management does not just "take place in a context of the objectives and activities", whatever that means.

Issue: is this all there is to context?

The first two sentences of section 6.3.3 of the Standard are partially correct in that the specific context for a risk management activity is derived from the overall context. However, this section fails to build the critical linkage between the scope and establishing the context. Understanding the problem space and then developing the scope helps to define what aspects of the overall context need to be examined as part of the risk management process. Without a scope, the context cannot be established effectively, whilst understanding the context helps to refine the scope in turn.

The second sentence of this section states: ”The context of the risk management process should be established from the understanding of the external and internal environment”. This is a somewhat clumsy sentence, and just what does the “context of the risk management process” mean? It appears that what the Standard is trying to say is that out of the overall context, there are parts that are relevant to the specific risk management activity being undertaken, and by extension there are parts that will not be relevant to the current activity (but may become relevant for future risk management activities). However, the Standard is opaque about how one considers the “external and internal contexts”, and then establishes a more specific context that will inform the risk management activity.

Section 6.3.3 also provides three dot points about why understanding the context is important. Combined, these dot points only attempt to justify understanding the “internal context” completely disregarding the “external context”. Even then the dot points are somewhat misleading. The first dot point states that “risk management takes place in the context of the objectives and activities of the organization”. This vague statement is difficult to understand, and can be interpreted in a number of different ways.

In the second dot point of the section, it states that “organizational factors can be a source of risk”, which seems to be just another way of saying consider the internal context. Again, it is not just the internal context, but the internal and external context (including how the two interact) that are sources of risk.

The third dot point in this section (“…purpose and scope of the risk management process may be interrelated with objectives of the organization as whole”) is similarly vague and clumsy. Is this trying to say that the purpose and scope is derived from these organisational objectives? That the purpose and scope cascades from the organisational objectives (akin to sub-objectives)? That if the organisation changes, then the purpose and scope of risk management also changes? Or does it mean that the purpose and scope are established so that they are consistent with and not antagonistic towards the organisational objectives. It may even mean that the risk assessment is specifically looking at the plans, progress or performance towards achieving some particular objectives. Alternatively, it could simply mean that organisational objectives should be understood and considered when establishing the purpose and scope for a particular risk management activity.

The final sentence of this section says that the lists of factors in section 5.4.1 of the Standard should be used to establish the “internal and external context”, but completely misses the point that it is those factors that are relevant to the specific risk management activity that should be considered. It is also not just the factors, per se, that are important, but also how these factors interact.

These lists also miss out important considerations about:

- The nature and rate of change that may be occurring in the context.
- The speed with which interactions with the organisation may occur, be detected, or could adversely affect the organisation.

- The time required for the organisation to respond once such interactions are detected.
- The extent of uncertainty that exists about the context.
- The potential for contagion effects to manifest, and the speed with such contagion effects would spread and cascade.
- The extent of dark data that may exist, but has not been satisfactorily identified.

Furthermore, for some reason only one of the dot points singles out that these are *effects on objectives*, a major omission since this is so central to the Standard's current definition of risk. Hence, all of the listed factors must influence or effect objectives ultimately, or they have no relevance for risk!

Resolution

An alternative approach for consideration during the revision could be to state that understanding the context is important because it:

- Provides us with the information to test the assumptions that we have made about the problem space.
- Establishes the systems and conditions, and their interactions, that can have causal influences on wanted and unwanted occurrences for the organisation.
- Helps us to both reduce uncertainty in our understanding and to recognise areas of remaining uncertainty that need to be addressed.
- Provides us with data that forms the basis of our analysis on which decisions are subsequently based.

Issue: confused about criteria?

Section 6.3.4 of ISO 31000:2018, covers "Defining risk criteria". The way in which this section is currently written has been a source of confusion for some practitioners, particularly about what these criteria are and when they are 'designed'. The following points require some simple clarification:

- In the 'Foreword', the 'principles' are identified as the 'criteria' (for successful risk management), and hence could be assumed by some readers to constitute the 'risk criteria'. This can be simply resolved by not using 'criteria' to refer to the 'principles'.
- Section 5.2 (Leadership and commitment) refers to establishing the criteria. It is unclear if this is an indication that criteria should be initially established as part of the overarching framework. This would make sense as it would establish the baseline on which individual sets of criteria could be modified for use in different contexts. This would also help in building consistency and comparability across different uses of the risk management process within an organisation. This needs to be clarified.
- If the intention is for the 'design' of risk criteria to occur as part of the risk management framework, then section 6.3.4 is not in the correct place within the Standard, and should be moved under the 'framework' section.

- This would then require a new section to be written on the *modification*[84] of risk criteria[85] based upon the scope and context of each individual application of the risk management process. This new section should provide guidance on why and how criteria can be customised, and the approach to be taken to validate this customisation, including surfacing and testing assumptions.
- Hence risk criteria may be different in different uses of the risk management process, for example as the context changes, for different applications, or for use at different levels of an organisation. Where such changes to criteria occur, this could introduce complications in comparing, prioritising, or aggregating risk from different uses of the risk management process. There will, therefore, be the need for guidance on methods for combining, aligning, aggregating, and interpreting the outputs of different applications of the risk management process.
- Section 6.3.4 also refers to risk criteria as "dynamic". This is incorrect, as risk criteria are not 'dynamic'. The word 'dynamic' means *constant change*, we certainly do not want risk criteria that are constantly changing. Whilst the context may be dynamic, modification of the risk criteria has eventually to set to enable their use. Criteria may need to change due a changing context or changing risk management objectives, based on *conscious informed decisions* of the 'analyst' [86]. Such change is anything but dynamic, otherwise it would be impossible to achieve any consistency in risk management and decision-making. Perhaps the standard is confused about the meaning of 'dynamic', the context and in particular the risk sources may very well be dynamic, but the criteria are most certainty not, as it would not then be possible "to set risk criteria" [87]. In other words, criteria may be 'flexible', 'mutable', or even possess some 'fluidity', but they are not dynamic.
- The very first sentence of this section states that the organisation should "specify the amount and type of risk it may or may not take", this will not in practice be the first criteria to be developed. How can one specify the type and amount of 'acceptable/unacceptable' risk before we know what criteria we are going to use to estimate or measure the risk (which is the second described activity in the paragraph). The order of the list needs to be rearranged.
- The Standard has frequent mentions of risk criteria, scattered about the document. These should all be consolidated into either the 'design' or a future 'modification' section if introduced.

Section 5.3.4 provides a list of considerations for setting risk criteria, which whilst giving relevant 'pointers' lacks sufficient detail to provide adequate guidance to the reader. Specific issues include:

[84] Note that modification may include changes to the nature of the criteria themselves, changes to any weight or importance attached to individual criteria, changes to the way that the criteria are measured (e.g., from direct observation of the whole data to observing only a sample, or changing the nature of the data collected), changes to metrics and values attached to individual criteria etc. This modification may include adjustments made to existing criteria, or the introduction of additional criteria.

[85] Such modification should not only occur early in the risk management process, but may require further modification should any changes occur that affect either how risk is assessed or how acceptable a risk may be.

[86] Or other authorised and competent person.

i) "Set risk criteria…"

This section of the Standard also provides a list of considerations to "set risk criteria" [88]. The word "set" is commonly used to mean to put something into place (where it will remain). However, the list provided is not about setting the criteria, but instead provides further consideration for the *design or creation* of these criteria. Nowhere in the Standard is there consideration of 'setting the risk criteria', an activity that should include considerations such as the final testing, validation and approval of the risk criteria, concepts that are not mentioned in the Standard.

Resolution

The title of this section is "defining risk criteria", which requires greater clarity and should include additional activities, including:

- Identification of requirements for risk criteria (aligned with the objectives of the risk management activity),
- Agreement on the decisions (and the information requirements for making these decisions), for which these criteria will provide a foundation.
- Selection of the types of criteria to be used.
- How the design and setting (validation and approval) of the risk criteria can be undertaken.

ii) *"The nature and type of uncertainties…"*

The Standard states that the "nature and type of uncertainties" should be considered in 'setting'' the risk criteria. At first glance this seems like a reasonable statement, however, it is vague, and lacks sufficient guidance. We have tested the understanding of this statement with tens if not hundreds of risk practitioners since the Standard was published, and only a small handful were able to provide a meaningful explanation of this concept.

The whole concept of uncertainty is complex. The vast majority of 'risk practitioners' only think about a very small range of different types of uncertainty when conducting risk assessments, and often only consider aleatory uncertainty (see below), whilst being unaware of, or ignoring other types of uncertainty. It is one of the major inadequacies of ISO 31000 that so little guidance is provided about uncertainty (Aven and Ylönen, 2019).

Although uncertainty can be defined simply as "that which is not precisely known" (Booker and Ross, 2011), uncertainty comprises multiple dimensions, attributes, and perspectives (Walker et al, 2016; Han et al, 2011; Liu, 2011)., and multiple different models have been developed to try to explain uncertainty (Chuilá and Uribe, 2019; Ülkümen, et al, 2016; Bland and Schaefer, 2012; Brugnach et al, 2010; Sainsbury 2009; Seymour et al, 2007; Yu and Dayan, 2003; Regan et al, 2002; Van der Heijden, 2002;1996; Lipshitz and Strauss, 1997).

[88] "set the risk criteria" is an instruction in the third paragraph of section 6.3.3.

A short discourse on uncertainty

To be effective, risk management should consider uncertainty in different ways (as always depending upon the context):

- There may be uncertainty about the past, the present, and the future.
- Uncertainty may be factual (the way the world was or is now) or counterfactual (the way the world could be if certain conditions are changed).
- There may be different 'sources' of uncertainty[89]:
  - aleatory uncertainty, arising from randomness, is addressed through applying probabilities (or likelihoods);
  - epistemic uncertainty, arising from an insufficiency of knowledge, is often addressed through non-probabilistic methods;
  - model uncertainty, arising from the risk model that is developed for an assessment (Xia et al, 2017). Because the model is an abstraction of reality, in creating this simpler perspective some pertinent information may have been excluded from the model, intrinsic errors incorporated, etc., which introduce additional uncertainty;
  - ontological uncertainty, which occurs when an artefact is newly introduced into a system and creates unfamiliar effects.
- There may be uncertainty that relates to how we make sense of and apply knowledge in making decisions (Sotani and Izquierdo, 2019; Dewulf and Biesbroek, 2018; Dosi and Egidi, 1991): e.g., subjective uncertainty (making assumptions and inferences when data is unavailable or insufficient); substantive uncertainty (e.g., relating to decision content); strategic uncertainty (e.g., actions of others following decisions); and institutional uncertainty (e.g., about the rules involved in decision-making).

In addition to uncertainty that may arise from the nature of the risk model that has been developed, other aspects of the risk management process may also introduce further uncertainty (Gibson and Gibson, 2023a) including:

- Issues around validity, integrity, accuracy, and currency of data and information sources.
- Natural variation and sampling error in the data collected.
- The nature of the analytical approach, its relevance and fit, precision, ease of manipulation (intentional and unintentional), introduction of artefacts, etc.
- Construction of risk scenarios, for example, their comprehensiveness and plausibility.
- Interpretation of analytical outputs, analytical capability (knowledge, experience, and integrity), biases, problem complexity, etc.
- Monitoring effectiveness, e.g., suitability of indicators, influence of data noise, timeliness, etc.
- Communication and reporting approaches, e.g., recognition and acceptability of channels and information presentation.
- Interpretation and use of risk management process outputs.

It is not just the type and source of uncertainty that should be considered, since different levels of uncertainty (Walker et al, 2013) may also affect the conduct of the risk management process (Figure 6), and necessitate the use of different tools and techniques within the process.

[89] The vast majority of both qualitative and quantitative risk assessment is based upon the assumption that uncertainty is either aleatory or epistemic, and in doing so ignores other types of uncertainty which could have profound influences on how risk is assessed (Blockley, 2013).

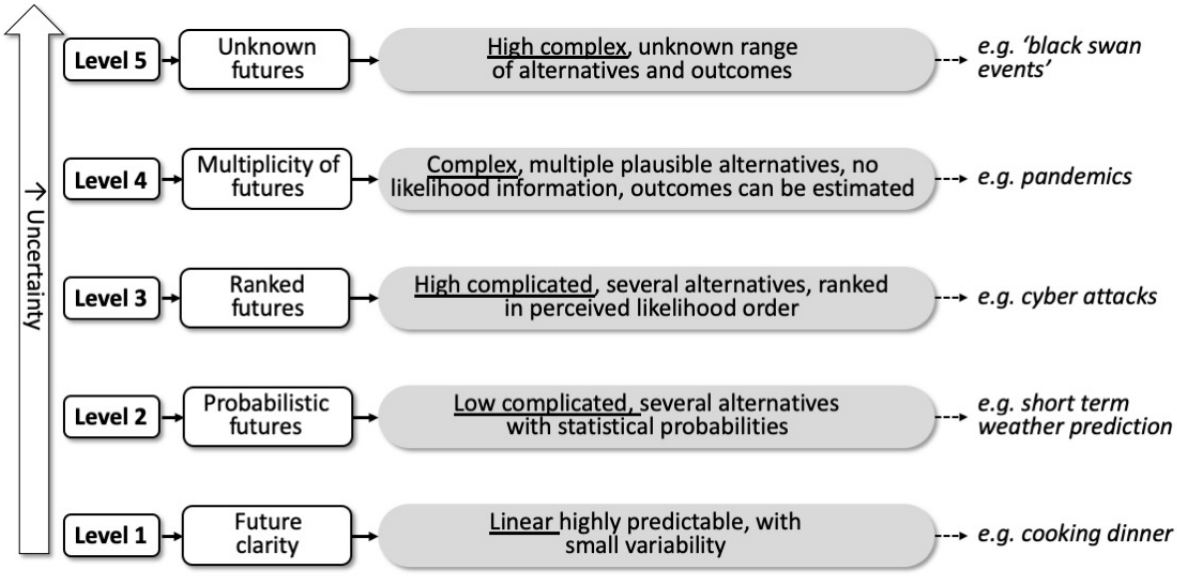


Figure 6: Levels of uncertainty[90]

Uncertainty is at the very centre of our understanding of risk (according to the ISO 31000:2018 definition) and at the centre of risk management. With uncertainty being so central to the definition of risk it is surprising that the Standard (outside of its definitional use) only mentions uncertainty in a single general sentence under the 'framework' section. With no mention of uncertainty at all in the risk management process sections.

Resolution

The next version of the Standard needs to include a more comprehensive discussion about uncertainty, including an explanation of uncertainty, the relevance of uncertainty to risk management, the reduction of uncertainty in decision-making, etc.

[90] Reproduced form Gibson and Gibson 2023a, with permission

The section on the risk assessment process

Section 6.4 ("risk assessment") of the Standard is probably the most widely referred to part of ISO 31000, and unfortunately is perhaps the only bit of the Standard that many 'practitioners' actually apply in their work.

This Whitepaper has already highlighted the key conceptual and practice flaws with the risk management approach as it is described in earlier sections of the Standard, and these comments also apply to section 6.4.

Issue: is this really how we identify risk?

The opening sentence of section 6.4.1 states that "the purpose of risk identification is to find, recognize and describe risks that might help or prevent an organization from achieving its objectives". Given the definition of risk, this is a tautological sentence (the effect on objectives is already included din the meaning of risk)[91], which requires rewriting because the purpose of "risk identification" is simply to "recognise and describe risks".

The second paragraph states that there are a range of techniques for identifying uncertainties, but neither provides guidance on what those techniques may be or how identifying uncertainties translates to identifying risk. Nor does this section provide any indication of how to decide which technique to use under what situations.

Risk identification has to involve, even if it is conducted intuitively, some form of causal reasoning and modelling. No one sees the release of a new piece of technology and then thinks "oh that could result in us losing 50% of our revenue in the next 5 years". Instead, they will imagine how that technology could develop in the immediate future, how that technology might be applied, how the organisation might respond to the technology's availability, how it may fit into their R&D program, the possibility that their competitors might adopt the technology, how customers would respond to this technology, etc. From such cause-and-effect reasoning we could construct a risk that "by not immediately investing in this technology we will lose our competitive advantage, resulting in a critical loss of market share within 2 years" and "by managing this risk we not only maintain market share but could gain a significant competitive advantage, that will double market size and revenue within two years, and correspondingly diminish market share for our competitors".

The Standard's description of risk identification fails to consider the importance of causal reasoning or provide a process or scheme for determining how 'sources of risk' may be identified, and how potential interactions between these sources and the various organisational interfaces can be recognised and mapped. An understanding of the nature of these interactions forms part of the construction of a collection of risks, but the Standard is opaque on how this could occur. Discussing risk identification in this way may seem strange to some 'risk practitioners', because our personal observations of common practices are that on many occasions risk identification relies more on intuition, than on a rigorous process of exploration that is melded with a deep understanding of the context.

[91] And if these 'risks' did not affect objectives, then according to the ISO 31000 definition they could not be risks!

This section of the Standard also provides a dot point list of 'factors' to be considered, but the Standard is not explicit on how these factors can be applied. Whist there is nothing technically incorrect with this list, it is somewhat limited, is inadequately constructed, and is unclear how it should be used. Following the first dot point "…sources of risk", all but two of the succeeding dot points are not separate considerations, but are simply just examples of "sources of risk":

- "causes and events".
- "threats and opportunities[92]".
- "vulnerabilities and capabilities[93]".
- "changes in internal and external context".
- "the nature and value of assets and resources".
- "limitations of knowledge and …information…".
- "time-related factors".
- "biases, assumptions and beliefs of those involved".

Of the remaining two factors in the list, "indicators of emerging risk" are just signals for certain sources of risks, and "consequences and their impact on objectives" is more usually associated with the Standard's 'risk analysis step' (and in fact is pretty much repeated in that section of the Standard). The way in which the list is written currently ("consequences…") is not a source of risk. Although the consequences of a particular risk could serve as 'sources' for a different risk. However, this is not explained in the Standard.

It should be noted is that this list of factors is not just restricted to use for "identifying risk", but may also be important consideration in the analysis of those risks. This further illustrates that "risk identification" and "risk analysis" cannot be conducted as two separate sequential steps. The two are far more intimately intertwined than the ISO 31000 process recognises.

Although, what we should now recognise as a list of risk sources (and not just "factors") is a reasonable starting point, what is actually in the Standard is still fairly vague, requires more explanation, and is still far from being comprehensive (for example, somethings as obvious as 'hazards', 'decisions', and 'plans' are omitted in the Standard's consideration). However, no matter how good this list of 'factors' could be, without the inclusion of causal reasoning into the process, we will still be left with just a list of 'factors', not guidance for identifying *risks*.

There is a highly concerning misconception, that the Standard perpetuates, of using the words 'threat' and 'opportunity' together as though they were antonyms (paired opposites). Opportunity is not the opposite of threat (yes, we know that SWOT analysis uses threats and opportunities, but that is still no excuse, 'risk practitioners' should know better). An opportunity is a set of circumstances that may allow something to be done, for example to pursue something of value. All opportunities have uncertain outcomes, i.e., all opportunities have risk associated with them, and pursuing an opportunity may result in gaining benefits, suffering harm, or a combination of the two. Whereas a threat is a source of risk[94], where the overwhelming balance of consequences is negative.

[92] "threats and opportunities" are often inappropriately listed together like this as antonyms, and frequently mislead the reader. Opportunity is not the opposite of threat. A threat is a change or 'thing' with the potential to cause harm. An opportunity is a set of circumstance which offer the chance of achieving something of value, but is also accompanied with a chance of loss.

[93] vulnerabilities and capabilities are also important considerations in control effectiveness.

[94] An opportunity is not a source of risk per se, but the circumstances, decisions, and actions associated with the opportunity and its pursuit are sources of risk.

Another of the several inconsistencies between different parts of the Standard, needs to be pointed out in section 6.4.1. One of the underpinning principles of risk management (according to the Standard) is the use of "best available information". However, for the risk assessment process, this appears to be inadequate, as this section of the Standard states this "best available information" now has to be supplemented with other information. The information is either "best available" or it is not, anything else is superfluous.

Emerging risk

The list of "factors" includes the concept of "emerging risks", which is the playground of much misinformation, and misconception. There is no clear definition or agreement about what constitutes an 'emerging risk', and much of what has been written is misguided and confusing. Due in large part because the term 'emerging risk' is used to mean many different things in different disciplines (and often within the same discipline), a proportion of which definitions are conflicting or mutually exclusive concepts.

Accordingly, attempts at producing an ISO Standard on emerging risk in recent years were heavily contested and ultimately doomed, and the compromise, the publication of a technical specification looks unlikely to provide any wide acceptance or satisfactory resolution.

The insurance sector often publishes reports that identify so called "emerging risks" simply describing them in terms such as "AI", "climate change", "natural resources management", "cyber risk", "pollution", etc. (for example, AXA, 2023). Firstly, none of these example are risks (if we are to be consistent with the ISO 31000 definition, or many of the scientific definitions of risk), at best they are potential sources of risk (hazards and threats), to be a risk they have interact with something and have an effect on something.

Secondly, what makes these examples 'emerging'?

With the exception, possibly of artificial intelligence, many organisations will have included a majority of these published 'emerging risks' on their risk register for at least the last couple of decades. Being aware of and analysing certain risks, over a twenty year period, hardly seems to qualify them as 'emerging".

It also seems that a lot of confusion about 'emerging risk', comes down to a basic misunderstanding about the nature of risk itself. A lot of the time when people are talking about "emerging risk", what they are actually concerned about are *emerging conditions* causing 'unexampled change'[95], which may then affect an organisation. Commonly, "emerging risk" is also used to mean risk that we should have been aware of, but have effectively ignored up to now. The term is also used where knowledge about the risk is sparse (Renn, 2014), that is we may have recognised the risk for a long time, but we just don't really understand what it is all about, or its character is changing significantly. At other times 'emerging risk is used to describe risk where its, consequences probabilities, or importance is accelerating faster than expected.

'Emerging risk' is in the eye of the beholder, what is emerging for one organization (or even in certain areas within an organization), may well already be just a 'risk' (assessed, understood, and treated) in another organisation.

[95] Not previously experienced.

With so many different meanings, the term "emerging risk" is either better not to be used, or when it is used, it needs to be accompanied by qualifiers to make certain that the reader understands its meaning.

Resolution

The section on risk identification needs to be substantially revised to take account of the issues raised above and to provide guidance on how risk identification should be approached in what are increasingly complex strategic and operational environments. Much of the current ISO guidance (in this Standard and in other publications such as ISO/IEC 31010) is restricted to traditional risk identification approaches, a great deal of which are decades old and do not reflect more contemporary analytical thinking. For example, risk identification could benefit from utilising insight gained from other organisational activities such as enterprise architecture, management of change, design thinking, data analytics, etc.

Issue: a weak analysis?

Section 6.4.3 of the Standard deals with what should be the wide ranging subject of risk analysis in about half a page. It provides some general discussion about risk analysis, but with little information about the different approaches to analysis, with no indication of what even a generic risk analysis process should look like, or any discussion about the nature of the outputs of analysis. There is little factually incorrect with this section of the Standard, it is just very short on useful conceptual and practical guidance.

There is a particularly relevant statement in the first sentence of the section "…purpose of risk analysis is to *comprehend* the *nature of risk and its characteristics*, including *where appropriate* the level of risk" (our emphases). This is very clear about what risk analysis is for, it is to deeply understand the nature of risk[96], and that this *may* include determining a level of risk – *in some situations*. Yet rating risk is almost universally seen as the reason for undertaking an analysis[97], the analytical product is almost always a rating of risks. Very few risk analyses provide a rich story, a narrative that describes the complexity of risk under consideration.

The crux of this concept is the Standard's very deliberate choice of a single word "*comprehend*", this is not just a fancy synonym for 'understand', "comprehend" means so much more. For example, we can all '*understand*' that flicking an electrical switch results in the air conditioner working, but do we really *comprehend* how electrical energy 'flows' through the wires, and how this energy interacts with the technology in order to cool down the room? Most organisational risk analyses seek to *understand* enough to assign a consequence, likelihood, and risk rating. Far fewer try to sufficiently *comprehend* risk in order to develop a rich narrative that explores the risk.

The second sentence in this section of the Standard also indicates the need to have a variety of analytical tools at one's disposal that can be applied to different scopes and purposes. Again, this is not something that we commonly see, rather a majority of 'risk practitioners' seem to use the exact

[96] The second sentence of section 6.4.3 provides a little more explanation of what is mean by the "nature of risk".
[97] In our observations across many different industry sectors, the most commonly encountered risk analysis output is a simplistic combination of consequence and likelihood to produce a rating or level of risk.

same analysis methodology for every analysis they undertake, with little conscious recognition that more optimal approaches are available.

The bullet point list in this analysis section of the Standard does provide a basic set of starting considerations, although it is not comprehensive, and is still fairly vague. The dot points seem more to be 'headings' for (missing!) sections, rather than providing informative guidance. It appears that whilst the first two dot points (about consequence and likelihood[98]) are loosely followed by almost every single risk analysis. Whereas the remainder of the list is partially observed[99] or completely ignored in practice.

The first dot point in this list provides the core of the risk analysis process, but is frequently misunderstood. A great many risk analyses (and 'analysts') simply 'get' the relationship between consequence and likelihood wrong, especially in qualitative analysis. The authors of this Whitepaper have lost count of the number of analyses where the likelihood of a base *event* has been combined directly with a consequence. For example: "there is a high likelihood that someone gains unauthorised access to client personal data" (the event), and "the consequences (damages against the organisation and reputational harm are high level consequences"), with a not uncommon conclusion being "therefore a high likelihood and a high consequence equals an extreme risk". However, read the first dot point in Section 6.4.3 very carefully: "the likelihood of events and consequences". Misunderstanding the concept that the Standard is trying to make, can result in some wildly inaccurate risk assessments. Combining a consequence with the likelihood (or probability) of an event, is not the same as combining the consequence of an event with the likelihood of those consequences occurring. By way of another example, consider a simple scenario (Figure 7):

- Janet, a single mother is late leaving for the railway station to catch a train home and decides to run down the street, with a chance of tripping and falling to the ground.
- With her choice of footwear, there is a 20% probability (p=0.2) that she trips and falls.
- A fall could result in a severe head injury and hospitalisation. The total combined consequence of her accident is calculated at $2 million.
- With the not uncommon (but incorrect) use of: 'event probability' X 'consequence', we would obtain a risk value of 0.2 X 2,000,000 = $400,000.

However, if we look at the (hypothetical) accident statistics for people running and falling:

- The vast majority of people that trip, do not hurt themselves.
- Of those few that do injure themselves, the vast majority receive little more than grazed knees and hands.
- It is very rare for someone to receive a serious head trauma.
- In our example we have also included the consequences that flow from a potential head trauma, which have an even lower probability p= 10^{-7}.
- There are a series of valid consequence x probability pairs[100] from which the risk could be calculated, e.g.:

[98] On the assumption that the word 'likelihood' was also meant to include probability in the Standard.

[99] Although many risk analysis includes some consideration of 'control effectiveness', the rigour with which controls are examined varies widely. It is not common to see a deep testing of controls (individually and as part of a system) to be undertaken, and even less common to see tools such as vulnerability analysis (determining the performance and weaknesses of controls under different potential future conditions) and control failure point testing (determining the circumstances under which a control performance will cease to be acceptable)

[100] Risk occurs as a distribution of consequences and probability, and although we can select various 'pairs', more appropriate calculation is achieved using various statistical tools on the distribution.

- the risk of tripping with no injuries, p=0.99: 0.2[101] x ($1[102] x 0.99) = $0.20
- the risk of tripping and receiving a minor graze to a knee, requiring minimal first aid, and 10 minutes lost work time, p= 0.099: 0.2 x ($11[103] x 0.099) = $0.22.
- the risk of tripping and receiving a serious head trauma, extended medical and rehabilitation care, and other losses, p=10^{-7}= 0.2 x ($2,000,000 x 0.0000001) = $0.04.

We would see similar differences between the two ways of assessing risk if qualitative criteria where used. Yet the former approach still persists in some organisations and consultancies.

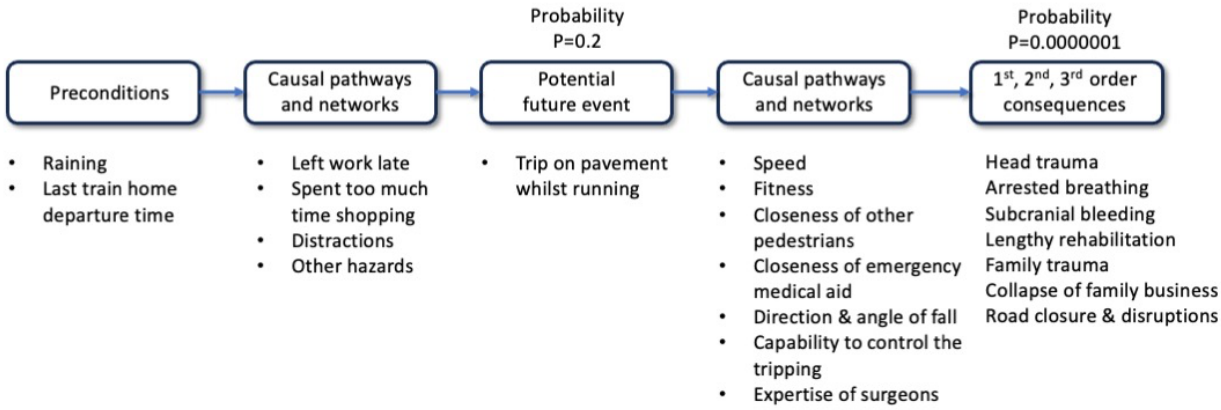


Figure 7: analysing risk – a hypothetical example

Thus, a likelihood (or probability) estimate should account for the likelihood/probability of the event occurring and the likelihood probability of the consequences occurring from that event either as single estimate, or as a conditional probability.

The silence on approach

A major problem with section 6.4.3 is that it gives equal weighting to qualitative and quantitative analyses, with the implication that either approach can be used effectively for the same 'problems'. Many commentators have made strong cases for abandoning qualitative analysis, and promoting the use of only quantitative techniques. We agree that in many risk analysis applications, qualitative *estimation* (often just 'guestimations') can produce very inaccurate, imprecise, inconsistent, and misleading outputs, compared with even simple quantitative measurements. Where the purpose of the risk assessment is to produce a value or level for risks, then there is a compelling argument that quantitative analysis should be used.

[101] The probability of initially tripping and falling
[102] The cost to polish out a minor scuff mark on shoe scrapped in the fall)
[103] Combined costs of 10 minutes lost work time, disinfectant, and sticking plasters)

However, we disagree with these commentators that there is no place for qualitative analysis[104]. Our opinion is that there are times when qualitative analysis can provide far more insight[105] than a technique that just produces a single numerical value (or a range of numerical values), so long as one understands when such techniques should be used, and comprehend the limitations of these techniques.

Resolution

The Standard must provide some guidance on how to make decisions about the choice of analytical approach, if we are going to move practitioners away from poorly thought out and often mathematically invalid methodologies. Irrespective of whether they are qualitative or quantitative.

Issue: what about human frailty?

ISO 31000:2018 appears to assume that humans (and in particular the human brain) is an expert and near perfect calculator of probabilities and consequences. Admittedly, there are two brief mentions of 'bias' in the Standard, and five occasions on which the word 'perceptions' are used. However, on each occasion that one of these words is used, it is only a single word mention simply dropped into a sentence or dot point, with no explanation of meaning, relevance, or influence of these concepts provided. 'Bias' and 'perception' are just two sources of cognitive error (O'Mara, 2017; Croskerry, 2014; Tversky and Kahneman, 1974) that can effect risk analysis.

It has been known for some time that individuals and groups are poor at estimation and calculation about situations outside of their experience, especially high-consequence/low-probability circumstances (Go-Science, 2012; Kunreuther, 2002, 1994; Woodell et al, 2002). So much so that the phrase "*managing risk through the veil of ignorance*" was coined (Marshall and Ojiako, (2013). However, the human brain is a particularly poor estimator and predictor of probabilities irrespective of the rareness or commonness of the situation (Maglio and Polman, 2016; Bilgin and Brenner, 2013; Browne and Brüne, 2012; Shermer, 2008).

In addition to the cognitive sources of error in risk assessment, there are other sources of error. For example:

- Arising from the type and nature of the data used.
- In the way that the data is selected, sampled, and collected.
- In the construction of the risk model and scenario.
- In the choice of analytical approach and tools.
- In the skill, experience and knowledge of the analyst, etc.

[104] For example, qualitative analysis can provide a deep narrative, that engages more areas of the brain than just providing numbers can achieve. Such qualitative analysis can provide a deeper understanding of the nature of risk and its interrelationships, trigger deeper pattern recognition, and facilitate deeper cognition for problem solving and decision making. Qualitative analysis can also provide an approach to address situations where data and information are limited, are ambiguous, are difficult to attribute, or are undergoing rapid change.

[105] For example, there are situations where it may be more important to understand the interrelationship across causal, contributing, and influencing factors, the nature of vulnerability, etc., than to provide a definitive level of risk. This may especially be the case when probability/likelihood are difficult, if not possible to estimate (e.g., with unexampled risk). Conversely it can also be argued that is possible to assign a measurement to almost anything in order to provide the basis for quantitative analysis (Hubbard, 2014).

Yet the effects of these errors on the accuracy and precision[106] of analysis are rarely considered by many practitioners (Hart and Cooke, 2013; Baynes et al, 2002), and as concepts are completely ignored by the Standard. Not only are these other sources of error not mentioned, but the whole concept of 'error' in risk assessment is completely ignored by the Standard. If one does not understand the extent and influence of error in risk assessment, then how can one even pretend to be performing any analysis or assessment of risk? In the absence of such understanding, risk assessment becomes simple guesswork.

Issue: of complexity and connectivity

In section 6.4.3 of the Standard, one of the dot points in the list identifies "complexity and connectivity" as important considerations in risk analysis, but again does not provide sufficient explanation of these two terms. Leaving the reader to again make assumptions about their significance and how to address them during risk assessment.

There is growing empirical experiential evidence of the difficulties of using ISO 31000:2018 as a sole methodology for exploring risk in non-linear complex contexts. One way of reducing the uncertainties associated with complexity is to transform the whole risk management approach into one which is more organic, reflective, and recursive (refer back to Figure 5). Although even using a relatively unmodified ISO 31000:2018 methodology, one can gain a great deal of insight just by better defining the interrelationships between the various risk sources, controls, risks, and treatments (Figure 8). There are a range of mapping techniques, such as bow tie diagrams, event tree diagrams, fault tree mapping, causal inference mapping etc (Peeters, et al, 2022; Ostrom and Wilhelmsen, 2019; Voicu, et al, 2018; Brewer et al, 2017; Rausand and Hoyland, 2004) that can be used for qualitative analysis, and easily modified for quantitative analysis.

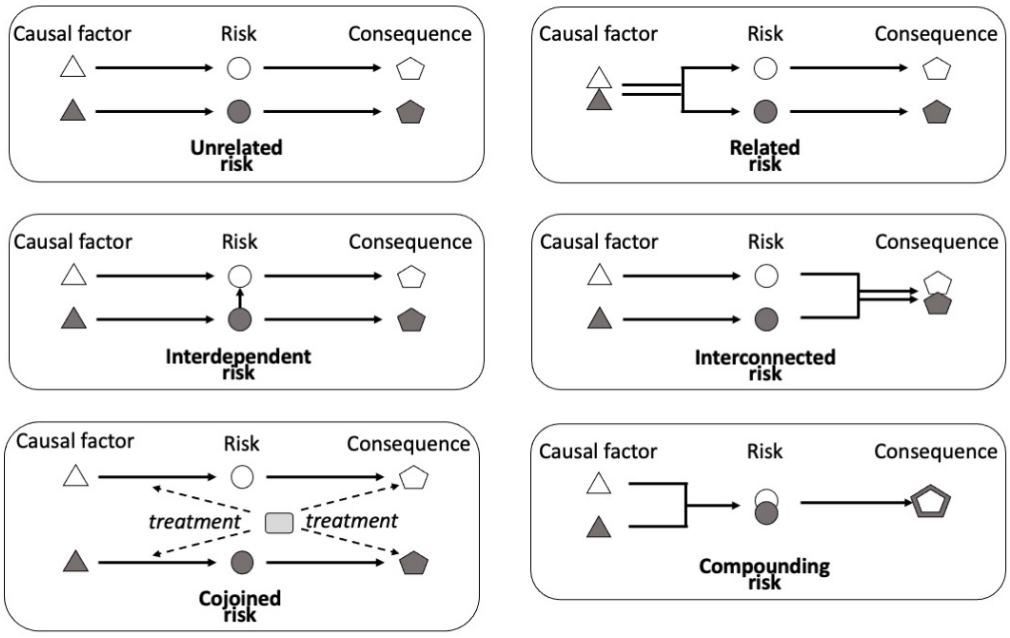


Figure 8: Risk connectivity[107]

[106] Accuracy refers to the closeness of the analytical result to the expected value, and precision refers to the amount of variation that occurs with repeated analysis of a risk (Kwon and Kang, 2019; Mun, 2014).
[107] Reproduced for Gibson and Gibson 2023a, with permission.

A related approach is to determine the relative importance and strength of the connections (degree centrality) amongst different risks (or between causal factors, controls, impact cascades, etc.). There are quantitative methods used to calculate degree centrality (Ashgarian et al, 2021; De Bruyckere, 2015; Stegiopoulos, et al, 2015), but an easier method is simply to count the number of outward connections (outbound centrality) and inward connections (inbound centrality) for each risk.

Using such approaches, the degree of connectivity between various elements (for example, risk connectivity – Figure 9), can be portrayed, and provides additional information on which to make decisions (beyond just using simplistic probability|consequence combinations). For example, in Figure 8 , a qualitative assessment would usually regard 'risk D' as the most important with a ' very high' (red) risk rating. However, when connectivity is considered, Risk Y (with a high outbound centrality) assumes a more prominent status, any change in Risk Y influencing change in five other risks (including Risk D.

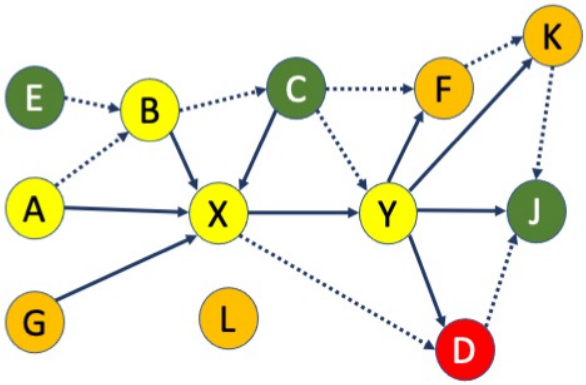


Figure 9: risk interconnections (hypothetical)

Resolution

The Standard should include a more comprehensive consideration of interdependency (across causal factors, controls and risks), and how interdependency can influence the nature and importance of risk beyond simple estimations of consequence and likelihood.

Issue: what has time got to do with it?

The fourth dot point in the list in section 6.4.4 of the Standard asks us to consider "time related factors and volatility". Again, this can be interpreted in a number of different ways.

Some consulting firms have realised that there are more dimensions to risk management than just consequence and likelihood, and have in recent years tried to persuade their clients to include a time dimension into their criteria. Some of the large consulting firms have gone further by releasing 'glossy' publications to promote their confected term of "risk velocity", which tries to (incompletely) capture the essence of the time issue (Quan and Chiang, 2017; Walters and Kluwer, 2017; Wolfe, 2014; Osundahunsi, 2012). There are several problems with the concept of risk velocity as used, and it is enough to irritate anyone that can remember their high school physics lessons, as well as anyone that uses the ISO 31000 definition of risk.

Those that promote the concept appear to not even understand what 'velocity' means. 'Velocity' is not just a fancier way of saying 'speed', the two are very different[108]. Yet the vast majority of the consulting firms and practitioners that use 'velocity' then go on to describe it as speed (Mohanty, 2020)[109]. Thankfully an error that ISO 31000:2018 has not made. The other irritation is that 'risk' (or uncertainty) possesses neither speed nor velocity. However, the conditions (that may be a source of risk) can be described as having a rate of change, and the forces released by that change may reach and interact with an organisation at different times[110], and their effects realised at different times. To think that risk itself can have velocity is a logical nonsense (given the definition of risk and its social construction). The concept would be better described as "context change rate", and "effect speed", but these terms are not nearly as sellable to a client. Even then, this is only part of the association between time and risk, and 'risk velocity' manifestly ignores some of the most important aspects of risk and time.

There are some groups that even tried to 'invent' a whole 'new' risk assessment methodology to encompass some time elements, calling it "dynamic risk assessment"[111] (Kristamuljana, et al, 2018) . We are unsure why some people regard this as new thinking, because (with the exception of using the term "risk velocity") many of us have been using a similar approach for decades, we just call it "risk assessment"!

It is also worth noting that the term 'dynamic risk assessment' has been 'borrowed' from emergency management, safety science, and from different areas of academia, where the term has been used and internationally accepted for many years to describe a quick assessment technique for first responders and safety professionals to use at the frontline (Cornelius, 2023; Li et al, 2023; Parhizkar 2022; EMV, 2021; Pozniak, 2011; Hornton, 2002). The existence of this well founded concept seems to have been ignored by consultants using this more recent confected use of the term.

Perhaps the most common consideration of time in risk analysis, is the time span of the risk scenario and context on which the analysis is based. For example, a project risk analysis may be considering the likelihood for potential future events and consequences (for example involving the loss of critical staff) occurring over the 18 month life span of the project. However, if the project has a five year life span, then consequence and likelihood may be every different. Changing the time period over which risk is considered can significantly alter the outputs of a risk assessment. However, it is a not uncommon practice for risk analyses to be conducted without defining such a time period.

[108] Speed is a term used to describe how fast an object moves from one point to another point and is a scalar quantity. Velocity, on the other hand, is the rate at which an object changes a position and is a vector quantity. This means that to use 'velocity' a physical direction must be included as well as the speed.

[109] Some consultancies do correctly define 'velocity' and 'speed' as different concepts, but then go on to try to measure speed and not velocity with respect to risk.

[110] For example, an external power transmission failure will be detected by an organization almost immediately; a wildfire may take several hours, after ignition, to reach an organisation's location; whilst floodwaters may take several days; each of these scenarios provide different warning periods and allow different times for preparation and response. Similarly, there will be different lengths of times before the various consequences reach unacceptable or disruptive levels (e.g., immediate disruption to operations from a power failure, to several days to weeks for a supply next work disruption to be realised from fires and floods).

[111] DRA.

Time considerations can also affect the importance of a risk in different ways. For example:

- How quickly might change occur?
- How quickly could this change transition from 'benign change' to 'adverse change'?
- How long would it take to detect this change?
- How long before we could make a decision about this change?
- How long would it take before this change would have an effect upon the organisation?
- How quickly could this change (or its effects) spread to other parts of the organisation, through the supply network, or to other interdependencies, or other unrelated organisations?
- How long before we could respond to the change?
- How long would it take to recover from the harmful effects of this change?

It is not common to see all of these issues fully considered in risk analysis, and reported to decision-makers. Too often all we see is a final risk rating product. One could find that a 'medium' level risk is less acceptable than a 'high risk', where that 'medium risk' comes with no allowance for early warnings, and the first awareness of the event is when serious harm has already occurred before it is detected.

Resolution

Making decisions about risk needs to not only consider the risk rating, but also the nature of risk (including its temporal aspects), and an organisation's ability to deal with that risk and its effects within the available time.

Issue: How effective are controls?

Determining the effectiveness of controls should be one of the critical inputs into risk analysis, but the manner in which this is approached varies widely from organisation to organisation, and even amongst individual risk assessments within the same organisation[112]. This includes:

- Effectiveness of controls judged on a qualitative (subjective) scale[113]:
  - as reported by the control owner/supervisor directly to the risk analyst;
  - following a management review of the associated process or specifically on the control landscape, reported to a third party and the information subsequently accessed by the risk analyst;
  - by direct inspection of control documentation (e.g., standard operating procedures), by the risk analyst or by independent audit;
  - by direct observation of the control operation by the risk analyst;
  - during an independent audit using *inquiry*, based upon reporting by the control owner, with the finding subsequently reviewed by the risk analyst;

[112] Based on the personal observations of the authors (in-depth reviews and ad hoc surveys of several hundred different approaches).

[113] Whilst independent reviews (such as internal audit) may use one or more of these control review approaches, unfortunately it is reasonably common for risk analysts to rely on a single control effectiveness estimate. However, when decision-makers use control information, they often perceive control effectiveness in a risk assessment to have an equivalent degree of rigour as that obtained from a dedicated independent review.

- by direct observation of control operation, or 'reperformance'[114] by independent audit;
- examination of historical control performance, errors, and breaches, conducted directly by the risk analyst or relying on the findings of third party independent review.

- Effectiveness judged on a quantitative measure, for example where process and control performance monitoring are conducted and recorded[115].

The vast majority of risk assessments (outside of industrial operational risk) appear to rely on qualitative evaluation of the controls, commonly expressing the effectiveness estimates by using qualitative rankings similar to Table 1.

Table 1: hypothetical example of control effectiveness rating and criteria[116]

Control effectiveness rating	Evaluation criteria
Fully effective	All controls are well designed, implemented, and modify the risk as required. Management believes controls to be effective and reliable. No further corrective or improvement action required, except monitoring.
Effective	Most controls are well designed, implemented, and modify the risk as required. Management is not confident that all controls are effective and reliable. Some minor corrective or improvement actions required.
Partially effective	Critical controls are adequately designed, implemented, and modify most of the risk but not fully to the required level. Management is concerned that key controls may not always work as required. Substantial corrective or improvement actions required.
Largely ineffective	Majority of controls are poorly designed, inadequately implemented, or ineffectively operated. Controls do not adequately modify the risk. Management has substantial concerns that controls are not working as required or fail regularly All controls require corrective or improvement actions required.
Non-existent	Controls are not in place.

In addition to any subjectivity involved in creating the inputs (e.g., from an audit review), the risk analyst will usually introduce additional subjectivity (and error) when using evaluation criteria such as those in Table 1. This subjectivity and error can be further compounded when the risk analysis aggregates control effectiveness across multiple controls into a single estimate (which is then used to help determine risk likelihood and consequence estimates).

[114] Involves auditors gathering direct evidence by operating the control themselves.
[115] Quantitative measures for controls are common in manufacturing processes, for some cyber, SCADA/ OT/ ICS and IT general controls for system and infrastructure performance. SCADA: Supervisory Control and Data Acquisition. OT: Operational Technology. ICS: Industrial Control System.
[116] Although Table 1 is a hypothetical example, it is based on actual evaluation ratings from several government and private sector 'best practice' guides. Note that the inclusion of this table is most certainly **NOT** a recommendation for its use.

These problems can be partially addressed by looking at the effectiveness of individual controls using more sophisticated tools. For example, for security-related risk, evaluating control effectiveness has been conducted for many years (Standards Australia 2023b) by specifically looking at control capability and effectiveness across the possible multiple objectives for a control, for example:

- *Detecting* change indicators (e.g., detecting an intrusion).
- *Deterring* an interaction (or its effects) with a risk source or threat vector (e.g., by making some controls visible, such as signage, physical controls, making people aware of rules, etc.).
- *Delaying* an interaction (e.g., preventing access, delegations, etc.).
- *Responding* to an incident (e.g., suspending access, investigations, contingency actions, etc.).
- *Recovering* from an incident (e.g., systems disaster recovery, insurance, staff welfare, disciplinary action, litigation, etc,)

Similar differentiated evaluation structures have been more recently adopted for other domains (IIA, 2023), looking at 'control relevance', 'coverage', 'strength/reliability', 'reactivity', 'resource availability', and 'exception analysis'. Whilst such approaches can help to provide a more informed insight in the nature of controls, they are still subjective techniques, and will be accompanied by some uncertainty and error.

Most control effectiveness evaluation approaches also have other limitations that need to be considered:

i) Control effectiveness is an estimate of the current performance of a sample of controls, operating under routine conditions. This rarely considers:
   - The completeness of the control suite.
   - How control effectiveness may vary over the life of the control or even over the 'life' of the risk (e.g., the period of time over which likelihood/probability is being considered).
   - How control effectiveness may vary in non-routine conditions (for example during an operational disruption).
   - Under what conditions control effectiveness may be unacceptably degraded.

ii) The criticality of individual controls, for example, some controls are absolutely vital (in their absence the risk would be wholly unacceptable), whilst other controls contribute although are not absolutely essential for modifying the risk. There are various criticality assessment approaches available (Standards Australia, 2023b; Gibson and Gibson 2023b; Márquez and Márquez, 2020; Paulsen et al, 2018) that seek to determine the *importance* of controls.

iii) Many major control failures, such as those resulting in crises and disasters, have been associated with fatal flaws (McKinnell, 2020b; Special Commission, 2020; Joint Investigation, Snow, 2018; 2016; van der Veght, 2015; Funabashi and Kitazawa, 2012; Holmes 2012; 2011 Halvorson and Hamilton, 2010; Parker et al, 2009; Stulz, 2009a; 2009b; Makinen, 2002) that were not picked up by standard control effectiveness reviews. A phenomenon known as 'normalisation of deviance' (Vaughn, 2016), explains how control operators can make unofficial 'temporary' alterations to controls to address local process difficulties that then become accepted practice over time.

These temporary fixes are not reported or captured in documentation, and although they work within the narrow limits of routine operations (also known as highly optimised tolerance), their effectiveness rapidly degrades and become highly fragile with even small

changes in operating conditions. Supervisors are rarely aware of the 'unofficial' changes, that have been made to controls, and routine independent reviews rarely identify them. There are often substantial differences (Figure 10) between 'work as designed' (how the control was originally meant to operate); 'work as imagined' (how supervisors and management believe the controls operate); 'work as reported' (what is officially communicated about the controls); and 'work as done' (how the controls actually operate).

iv) As most control effectiveness assessments are focused on inputs (e.g., the operation of the control against a documented procedure or standard) they can be especially prone to error because of normalisation of deviance. Even when control assessments are supplemented by testing and validating performance of the controls, they do not commonly reveal latent issues[117] (vulnerabilities) associated with controls, and where such vulnerabilities may emerge as conditions change. Vulnerability assessment aims to explore the presence and potential for such latency.

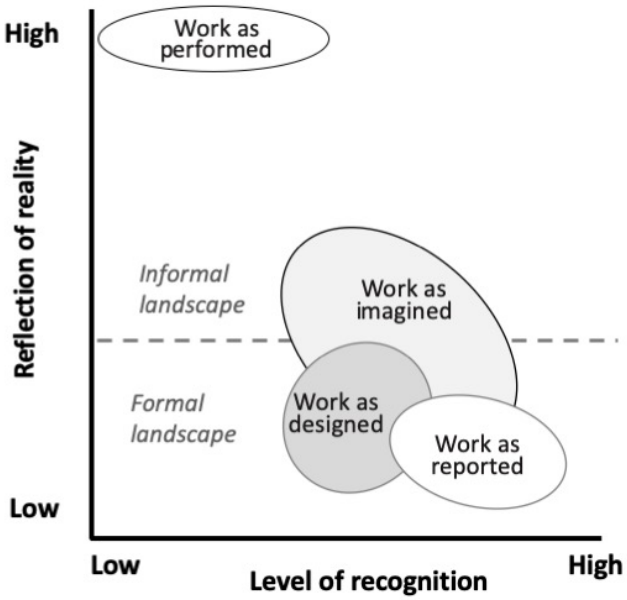


Figure 10: Formal and informal landscapes[118]

Resolution

The concepts of control effectiveness and control vulnerability require additional explanation in the revision of the Standard.

[117] Not all vulnerabilities will be 'latent' per se. Some vulnerabilities will be 'active' causing a current deterioration in control capability and performance, although in a way that may not be easily detected using routine assessment. Conversely, some vulnerabilities may not even be present during routine control operation, but could be introduced as the control (or control interdependencies) come under increasing stress as conditions change.

[118] Reproduced from Gibson and Gibson, 2023 with permission.

Issue: are we too sensitive?

Another area almost completely ignored by the Standard is the need for sensitivity analysis. The concept of 'sensitivity' has a single word mention (in section 6.4.3 of the Standard) in a dot point, with no explanation of the concept or its application.

Understanding risk is also about understanding the uncertainty surrounding the asymmetric effects of change. When parameters in our environment change, uncertainty means that it may not be immediately obvious what the effect these changes may have. This uncertainty can be further increased by asymmetric effects (small changes result in large impacts, whilst large changes may result in small impacts). Sensitivity analysis provides some insight into, and the ability to measure the effects of these changes through looking at the effects of alterations to analytic inputs and assumptions used to construct the risk model (Infrastructure Australia, 2021; ADB, 2010; Saltelli et al 2002). Using sensitivity analysis may also help to uncover risk that was previously unrecognised.

Although the main purpose of risk assessment is to unravel and address uncertainty in our strategic and operating environment, our biases, perceptions, and choice of analytical method can introduce their own additional uncertainty during an assessment. Accordingly, any 'risk result' that is produced will never be 100% accurate, there will always be uncertainty as to what the 'true' value is. An estimate or measurement of risk may be accurate enough as makes little difference in decision-making, or may have such uncertainty, that the error could 90% or greater (above or below) the value we report.

In our experience a majority of risk practitioners have little sense of the degree of error or confidence limits of the analytical tools and techniques that they are employing.

This is why the final dot point of the list in Section 6.4.3 of the Standard is so important, but unfortunately seems to be one of the least observed[119].

Resolution

Concepts of error, sensitivity, and confidence limits have to be explained in the Standard as vitally important considerations in undertaking risk assessment.

Any time that there may be uncertainty in the analytical data or results, this should be qualified by some expression of confidence in those results. In quantitative analysis, statistical measures, such as confidence intervals (e.g., there is a 95% probability that the 'true' result is somewhere between '+x' or '-x' of the reported mean value), confidence limits, or confidence levels (the % times that the same value would be obtained from repeating the analysis multiple times). In qualitative analysis, 'confidence statements' can be used to provide a subjective indicator of the analyst's confidence in the risk assessment outputs. For example, "this is rated as a 'significant' risk with a 'moderate' degree of confidence".

[119] Based upon personal observations of the authors, made across multiple different organisations, across multiple sectors, and involving 100+ different risk assessment approaches, less than 5% routinely include a sensitivity analysis.

Confidence in analytical outputs can be increased by:

- Repeating the analysis multiple times with different analysts.
- Repeating the analysis with the inclusion of additional tools and techniques.
- Repeating the analysis with fundamentally different analytical methodologies, including using more objective methods.
- Building causal models and determining causal inferences.
- Undertaking pre-risk analysis evaluation, for example, determining the accuracy of input data and the reliability of data sources (such as using the Admiralty System, Hanson, 2015), or assessing the strength of the knowledge that has been established during the analysis (Aven, 2017b).

Issue: dealing with biases and divergency

The analysis section of the Standard quite correctly points out that various factors such as divergent biases, opinions, assumptions, perceptions[120], etc., will influence a risk analysis. However, the Standard provides no explanation of these concepts or their relevance to risk assessment (or to risk management), nor any guidance on how the effects of these factors could be addressed. Although this section clearly states a problem, few risk analysts seem to have in place mechanisms to address these sources of variation in risk assessment.

This is a key issue in risk analysis, that has its source in the way that the human brain has evolved. We humans have a natural tendency to try to explain everything in terms of cause-and-effect, innately as a linear sequence. For tens of thousands of years, eruptions, floods, disease, earthquake, etc. would be perceived as being due to the people doing something that angered the gods, which then sent death and despair as divine judgement. Although a lot of the superstitious basis of this thinking started to be replaced during the 17th Century enlightenment in Europe, the simple linear nature of cause-and-effect was further strengthened (for example Newton's clockwork universe concept), and became firmly embedded into western culture up to the present time (now known as Cartesian-Newtonian thinking). In fact, Cartesian-Newtonian thinking forms the foundation for most contemporary risk management approaches (including ISO 31000:2018). However, there is increasing scientific evidence that such mechanistic linear thinking can severely distort perceptions of and decisions made about risk (Tepetepe, et al, 2022; Inghels, 2020; Dekker, 2015; Kleynhans and Spies, 1994). As well as being a source of a whole range of biases that will affect how we think about and assess risk.

The problems with Cartesian-Newtonian thinking can be partly addressed by avoiding the temptation to always trying to reduce risk information down to its individual component parts and addressing them individually. With complex situations, such reductionism can yield highly misleading answers, as one of the features of complexity is the emergence of new conditions and behaviours which are not apparent from looking at individual elements. What this means for risk management is that we have to try to model the interactions involved amongst the various identifiable causal, contributing, and influencing factors (often through mapping approaches) and gain insight through using causal inference techniques. These complex situations can mean that quantitative risk assessment is little better (or no better) than qualitative techniques, since statistical probability was never developed[121] to deal with such causal pathways (Pearl and Mackenzie, 2019).

[120] Remember that all risk is perceived.

[121] The early philosophers, including Francis Galton (the developer of statistical theories of normal distribution, correlation, and regression to the mean), abandoned or ignored causality concepts in their thinking.

There are a range of tools available that allow investigation of the influence of perceptions, biases, and judgments on risk assessment, such as the probabilistic functionalism of the Brunswikian lens (Dhami and Mumpower, 2023; Burgoon et al, 2022; Mear and Firth, 1998; Morina, 1994).

Resolution

Overall, the risk assessment section conveys the illusion that risk assessment is a simple linear process that can be satisfactorily undertaken by just following the superficial theoretical 'steps' described in the Standard. Any revision of the Standard needs to more deeply consider the way that risk assessment is carried out in practice, and in particular has to facilitate a better understanding of acceptable and unacceptable practices, including the limitation of specific approaches, as well the general constraints that apply across all approaches (such as the effects of biases and divergence).

Issue: what happened to aggregation?

One of the most confusing issues in risk analysis, and the one that is probably most inconsistently applied is the thorny question of how to combine different types of consequences. There are two considerations in this: how different consequences for a single risk can be consolidated, and how the consolidated consequences across different risks can be aggregated[122]. Two concepts that are completely ignored by the Standard.

Notwithstanding this omission from ISO 31000:2018, there is no other overall standard or best practice handbook providing guidance on risk consolidation and aggregation. Some sectors, such as banking, have adopted similar methodologies to bring together a high level view of overall financial risk exposures, but individual organisations apply different rules for the manipulation of data in aggregation (Inanoglu and Jacobs, 2009). Currently, risk practitioners are largely left to their own devices to resolve this issue. The result is that some ludicrous practices have been adopted, such as using the average qualitative value of a number of a different types of consequence or risks. For example, where a particular analysis provides 'medium' or 'low' level consequences or risks for 'financial', 'operational', 'external stakeholder' categories of risk, but a 'high' level for 'health and safety' risk. The analyst responsible then produces a consolidated *average* level of 'medium'. Yes, we have seen this nonsense in the risk assessment processes of a number of organisations, in each of which the analyst had little realisation that should the situation described by the risk actually occur, then someone would die (high consequence), not just a first aid incident (the 'medium' consequence), cumulatively added to which would be each of the other consequences.

The questions of consolidation and aggregation can be relatively easy to resolve in quantitative risk analysis, when different consequences can be converted into dollar amounts. However, the issue is much more complex for qualitative analysis.

[122] This also includes how different risks can be consolidated and aggregated across different parts of an organisation.

The qualitative consolidation problem

The analysis of an individual risk can produce impacts (values) across a range of different types of consequences[123], for example:

- Health and safety impact.
- Environment impact.
- Operational capability impact.
- Delivery schedule impact.
- People impact.
- Compliance impact.
- Reputation and customer impact.
- Financial impact.

Effective consolidation of these impact values requires that different consequences and impacts are mapped with respect to causal pathways and interdependencies. For example:

- If the event described by the risk scenario were to occur, would all consequences and impacts be 'automatically' realised to the same extent and within the same timeframe?
- Do some consequences and impacts have stronger correlations to other particular consequences, compared to others? For example, if the primary health and safety consequence occurs, will this also be accompanied by certain collateral levels of financial, operational, delivery schedule impacts (as well as the direct impact occurring from the event, e.g., damage caused to equipment – operational impact).
- Is there a greater 'sensitivity'[124] towards certain types of impacts compared to others, such that weightings could be applied to the values.

A factor that is often forgotten in consolidating multiple consequences (and impacts), is that each consequence has its own likelihood (or probability in quantitative analysis), which the consolidation needs to take account of.

Aggregating the values of different risks needs to consider similar issues to consolidation, requiring consistent principles and rules to be applied on how the values of multiple different risks are to be combined into an overall aggregated value. Whilst aggregation of similar risks can be complicated, aggregation of different risk types can be exceptionally complex, and requires additional analytical tools beyond simple risk analysis, to resolve.

[123] In many risk management approaches the terms 'consequence' and 'impact' are used synonymously, whilst in other approaches the two terms may be used differently. Practices that have caused some confusion. We use the term 'consequence' to describe the type of effect (e.g., a health and safety injury), and 'impact' to describe the measurable specific effects that arise from that consequence (e.g., loss of limb with permanent disability with $x thousand dollar compensation, costs of regulatory penalties, costs of disruption to production, legal defence costs, corrective action and rectification costs, etc.)

[124] 'Sensitivity in this context is used to describe the fear of, aversion to, or psychological amplification of perception of a certain type of risk. For example, a local community may have a higher sensitivity towards risk involving a spill of hazardous chemicals compared to a risk associated with flooding, although the latter may be result in far higher damage and would be more likely.

Resolution

The concepts of consolidation and aggregation of consequence and risk are persistent major problems in risk analysis, with many analyses relying on gut feel to establish an overall consequence or risk level. The revision of the Standard needs to incorporate guidance on the concepts of consolidation and aggregation, and on how this can be approached practically.

The section on risk evaluation

ISO 31000:2018 correctly states that "the purpose of this evaluation is to support *decisions"* (our emphasis). However, a significant number of risk practitioners assume or interpret this to mean to *make decisions only about risk treatments*. Whereas the intent of the Standard is to inform strategic, operational, and tactical decisions wherever appropriate in the organisation, and not just be limited to traditional risk treatment decisions. The key benefit of undertaking risk management[125] should be to ***reduce the uncertainty in making decisions***, not just attempting to reduce risk by modifying or adding controls[126].

Unfortunately, the dot point list in this section then rather ignores the earlier established broad remit for "risk evaluation" and instead has reinforced the narrow treatment-centric focus for evaluation.

Issue: the Standard has no appetite for risk!

One of the outcomes from risk evaluation should be a decision on whether a risk is acceptable or not, and then to address the implications of that decision. One of the criticisms, by multiple commentators, of the Standard is that it omits any mention of the concept of 'risk appetite' or of 'risk tolerance'[127], although does use the word 'acceptable' twice in reference to risk (section 6.5.1).

Irrespective of its omission from the Standard, the use of "risk appetite' statements has proliferated across corporate, government, and not for profit sectors over the last decade or so. The adequacy of the risk appetite concept has been challenged by an absence of a consistent definition for 'risk appetite', confusion with 'risk tolerance', inconsistent practice, and application of inappropriate performance targets, the absolutist setting of limits, and the disconnect between the presence of multiple stakeholders and singular risk appetites (Martens and Rittenberg, 2020; Ramamoori and Stover, 2018; Viscelli et al, 2017; Aven and Aven, 2015; Freund, 2015; Hillson and Murray, 2015; Cantemir, 2014; Gifford, 2013; Petria et al, 2012; Quail, 2012; Power, 2009), whilst many of the risk appetite definitions that do exist are either vague or inconsistent. All of which has contributed to a continuing disagreement over the benefits of extrapolating the concept into areas for which 'risk appetite statements' were not originally intended.

The use of risk appetite statements may make some sense and provide some benefit (Lee et al, 2022; Gontarek and Bender, 2019), in some circumstances. In the finance sector, establishing risk appetite appears to have been a far more exacting process than seen in organisations outside of the sector, with the result that the formulation and meaningfulness of non-finance related risk appetite statements have been questioned. This has resulted in a lot of these latter "appetite statements' unnecessarily occupying Board and senior management time, with little proven additional value. Although, it is possible that some conversations about risk appetite will have raised awareness about risk in general and may have provided some appreciation about what is and is not acceptable risk. Conversely, it is also likely that similar outcomes could have been achieved through discussions other than about 'risk appetite statements).

[125] And the overriding purpose of risk management.

[126] Which in many 'risk treatment plans' unfortunately involves addressing individual controls in isolation and independently of each other.

[127] The two very different concepts are often confused and the terms are frequently used interchangeably (Lope de Paula, et al, 2021).

It is a simple matter for anyone to access online and to review the risk appetite statements of a variety of different organisations (especially in the public sector). It should not be surprising that many such statements betray highly linear thinking, and ignore multiple other factors that are important in deciding if a risk is acceptable or not. It is then interesting to speculate about the extent that such 'motherhood' risk appetite statements contribute to poor decision-making.

It is also worth noting that much of the 'fad' for risk appetite statements in non-financial organisations ignores the science behind the concept of risk aversion (Rabin and Thaler, 2001; Pratt, 1964). Many risk appetite statements seem to have been developed without any formal consideration of the organisation's 'capacity' for that particular type of risk or direct alignment with its strategic and operational objectives (Manolescu, 2011; Alviniussen and Jankensgård, 2009).

There can be a great difference between establishing criteria which guide decisions about the acceptability of risk (which is of great importance) and establishing a risk appetite statement, which often becomes a vague rigid statement of historical preference (Jarvis, 2014), instead of looking at risk acceptability as a balance of risk and return. However, we have seen organisations that regard 'risk appetite' as a 'black box' gateway that replaces professional judgement, to the extent that discussions about and prioritisation of key success factors (Fraser, 2014) are lost to the risk evaluation.

If not fully motherhood, many of these 'risk appetite statements' are commonly unaligned with a whole range of other decisions that these organisations have to make about the acceptability of risk. Indeed, we have seen in multiple organisations where 'risk appetite statements' are in direct conflict with compliance requirements, organisational policies, risk criteria, or ignore risk acceptability limits that are implicit in various organisational business rules and instruments.

Organisations have been making decisions about risk acceptability for many decades (just not calling it 'risk appetite'), implicit and explicit within the policies, processes and business rules that it operates within[128]. Where these established acceptability limits can be extracted and summarised (or even consolidated), then fine, let's refer to them as 'risk appetite criteria'. But let's not get caught in the hype and the trap of trying to invent a risk appetite statement out of thin air, without reference to the range of implicit risk acceptability criteria that are already present in most organisations. Unfortunately, too many organisations have taken something that has a specific purpose in the finance sector (Govindarajan, 2011; Orros et al, 2011), and extrapolated it to purposes for which it was never intended.

The use of the risk appetite concept has been criticised on both conceptual and methodological grounds. Whilst the proliferation of risk appetite statements has arguably resulted in more simplistic decision-making being undertaken, increasing bureaucracy and a slowness to respond to change (Alviniussen and Jankensgård, 2019). In fact, there is little convincing published evidence that a 'risk appetite statement' improves the outcomes of risk management for non-finance sector organisations. In the absence of credible causal evidence, the value of investing precious time in crafting these appetite statements remains doubtful.

[128] For example: regulations, contracts, policies and procedures, delegation systems, business cases, process threshold values, business objectives, budget allocations for controls, all of the other risk criteria, crisis management triage system, business impact analyses, cost benefit analyses thresholds, decisions already made by senior management and the Board, community expectations, duty of care obligations, expected risk-reward trade-offs, investment guidelines, strategic and operating plans (e.g. objectives and performance indicators), behavioural norms and expectations, etc.

One of the major problems with the use of risk appetite statements that seems to garner little publicity or coverage in the literature, is that 'risk appetite statements' are highly static limits, and fail to reflect the dynamic nature of most organisations and their contexts. Neither does risk appetite (as commonly used) deal adequately with how sensitivity to risk and perception of value can change over time. For example, many organisations establish their 'risk appetite statements' at some point in the year, which then remain in place until the next associated strategy review meeting, which if one is lucky may be the same time the following year, but could be several years later. Consider the following hypothetical case:

- The risk appetite statement is written and approved in December to January.
- Over the previous 6 months the relationship with the key customer Acme has generated 80% of revenue. The assessed 'significant' risk of diversifying into new products and markets was judged to be above the organisation's risk appetite.
- In May, Acme decides to source alternate suppliers, with a predicted 50% drop in purchases from our organisation.
- Although the risk profile for diversification remains unchanged, the importance of such a strategy has increased due to the foreshadowed loss of future revenue. The risk-value balance has changed, and what was a previously unacceptable diversification-related risk is now much more acceptable. However, the static risk appetite statement no longer reflects the actual acceptability of risk.

In such a scenario, would we find it acceptable to be continuously rewriting risk appetite statements (which would be impractical on time and cost grounds alone), or would it be more effective to be able to adjust acceptability based on the risk criteria used to assess the risk?

Establishing acceptability criteria

It is important to have a consistent means of determining whether a risk is acceptable or unacceptable. For certain 'simple' risks this could be achieved by establishing acceptability based upon a threshold limit of risk (the philosophy behind many 'risk appetite statements'). However, there are many risks that are complex and require more than just a proximity to an arbitrary set risk rating limit. In such cases the decision-maker needs to consider more factors than just a quantitative or qualitative risk rating. The nature of the changing context, changing importance of objectives, the nature of remaining uncertainty, etc. may be as or more important influences (compared to the risk rating) in making a decision.

Every day we have to make decisions about the acceptability of risk, and our acceptability for that risk may change each and every time we make a decision, even if it as simple as the risks associated with crossing the road. If our perceived value from the crossing the road is sufficiently high, then we will cross the road even if the risk is well above our normal safety threshold. People make such judgements every time they think about crossing the road where they are, rather than walking a short distance further to a pedestrian crossing.

It is our view that the Standard's silence on the concepts of 'risk appetite' and 'risk tolerance', is probably appropriate. Since there is no agreement on what these terms mean, on how they can be established, or on the value that using such terms actually realises (Marshall, et al: 2018; Chapelle, 2016; Tophoff, 2014), then the use of the concept of 'risk acceptability' is far clearer, easier to define, and makes far more sense.

Resolution

Given that a key outcome of effective risk management is better informed sensemaking and decision-making, the Standard largely ignores how such understanding improves decision-making. This is an obvious area for the inclusion of a separate section in the revised Standard on 'decisions'.

In this respect, ISO 31000 really cannot afford to remain silent on making decisions about risk acceptability.

However, in order to limit any further contribution to the confusion and some pretty poor practices, the Standard should continue to avoid any content that attempts to explain 'risk appetite' and 'risk tolerance'. Instead, the revision needs to provide more informed guidance on criteria relating to the acceptability of risk, and in doing so it should suffice to simply state that there are no universally accepted approaches to defining 'risk appetite' and 'risk tolerance', and that these are just different perspectives on the acceptability of risk.

The section on risk treatment

Issue: another problem with iteration?

Section 6.5.1 promotes the use of a traditional linear process again, this time for undertaking risk treatment, by seeking to have the process 'iterative' (which means complete all of the steps in sequence, then repeat the process, again and again and again…). Whilst this can be an appropriate methodology for addressing simple linear risk with simple mechanistic treatments, it will be increasingly problematic as complexity in risk and complexity in the required solution increases. For risk treatment to be effective, it should consider:

- Alignment with and use of an organisation's existing project management methodologies and systems, where these are effective themselves (think about how many treatments will be designed and implemented in different parts of the organization, will these not involve the use of the organisation's project management processes?). Adopting such approaches can be especially beneficial in those organisations that have moved to more agile and adaptive project management methodologies.
- A decision-making framework to ensure that options analysis (refer to section 6.5.2 of the Standard) is robust and evidence based. In some complex situations, decisions about treatment options may require additional comparative risk assessments to be conducted for each of the individual options[129] (or suites of connected options), and incorporated into the cost-benefit analysis. For the selection of options to address complex problems, detailed quantitative modelling may be required, which may need to consider:
  - the level of risk modification achieved;
  - feasibility of design, development, implementation and on-going maintenance;
  - user and other stakeholder acceptance;
  - full life-time costs (including procurement, set up, roll out, training, approvals and permits, monitoring, maintenance, decommissioning, and disposal);
  - collateral exposures, risks, and costs created;
  - collateral impairment or enhancement of other controls;
  - additional performance benefits or degradation, life span and depreciation, etc.
- Design of the risk treatment requires an effective design process, and needs to be focussed on the user needs and utility. This will often benefit from a human-centric process (such as design thinking and human centred design[130]). Good design is often recursive, reflexive and reflective (rather than iterative) and involves testing designs with users, modelling, pretotyping[131], and protoyping[132] conducted before implementation.

[129] Remember that one of the outcomes of risk management is to reduce the uncertainty about each of the different options so that more informed decisions can be made.

[130] Refer to earlier discussions in this Whitepaper.

[131] Pretotype: A rapid experiment that aims to test ideas quickly, simply, and at low cost, gathering data in order to validate ideas *before* building a prototype. *Often run in a series, building on the learnings from each previous pretotype experiment to test each element of the proposed product.* A prototype asks the question: CAN we build it? By comparison, a pretotype asks: SHOULD we build it?

[132] Prototype: A first or preliminary version of something from which other variations are developed.

Issue: a muddled collection of options?

Section 6.5.2 provides a list of risk treatment options which are a little muddled, overlapping , and not always sufficiently clear. Treatment options can be more simply categorised by the following schema:

i) Treatments that modify the likelihood of a 'risk', including:

- reducing likelihood:
  - avoiding the risk (risk sources). For example, by not undertaking an activity that creates an exposure to the risk source, then the likelihood is reduced to zero,
  - removing or eliminating the risk source. For example, by, isolating a computer system from external networks, the threat of external hacking is removed, reducing the likelihood to zero. (Although, there will still be physical intrusion-related risk or a trusted insider-related risk),
  - diversifying operations, so that if one area of operation could be adversely affected by a situation, other areas are less likely to significantly affected;
  - other reductions in likelihood, such as controls that reduce the frequency of disruptive events, reduce the number of interactions with hazards and threats through other control improvements, etc.

- increasing likelihood:
  - creating or increasing the exposure to potentially beneficial situations. For example: bidding for more tenders (but in pursuing opportunity there may also be negative consequences such as increased direct costs, increased opportunity costs and other opportunities lost, distraction and loss of focus, etc.).

ii) Treatments that modify the consequences:

- directly reducing the harm, for example crisis management response, contingency measures, expenditure limits, loss control strategies such as stop-loss asset sell off points), etc.;
- distributing or slowing down the harm, for example delaying processing of orders, managing cash flow (for example by short-term increase of discounted sales, extending payment periods, etc), relocation of operations, hedging strategies, etc.;
- sharing the risk, for example offsetting part of the financial exposure through insurance, contracts, derivatives, other special financial instruments, etc.

iii) Treatments that retain or maintain the level of risk, for example retention strategies, accepting the risk but putting in place heightened surveillance, etc.

It should be noted that some treatment strategies affect the likelihood of the circumstances (risk sources) arising, some affect the interaction between the circumstances and the organisation, some affect the likelihood of the organisation being able to respond sufficiently, and some affect the likelihood of the consequences occurring.

Resolution

The Standard's consideration of risk treatment is overly simplistic and narrow, and is focused only on "risk-informed" strategies that provide traditional mitigation or exploitation options. The Standard completely ignores equally important treatment types such as "cautionary/precautionary" strategies

(robustness, resilience, containment, and research to improve knowledge), and "discursive strategies" (people involvement and awareness, confidence building and trustworthiness, further uncertainty reduction and clarification, increased accountability, etc.) (Hardy and Maguire, 2016; Aven 2015; 2014, Klinke and Renn, 2011; 2002; Renn, 2008; Aven, 2006; Renn et al, 2004) which need to be added to the above dot point list in the revised Standard.

The treatment section in the Standard also suggests that treatments need to be monitored for "unintended consequences" and the introduction of new risks (both of which are really the same issue). However, as noted above, it is as important that the prospect for treatment creating 'additional risk' is a consideration that occurs in the option analysis and the design analysis, and is not just left until after the treatments are implemented.

Issue: do we always need risk treatment plans?

Many ISO standards in the risk, security, and resilience spaces have a preoccupation with developing planning approaches that are *separate* from the rest of the organisation's activities. A focus on planning can also descend into a bureaucratic exercise, where plans are slavishly followed irrespective of how the context and organisational priorities change. For some simple treatments, traditional planning may suffice, whilst other types of treatment may require more sophisticated strategic or agile approaches (Seet, 2020; ASSNServices, 2018; Ahimnisibwe, 2017; Recklies, 2015; Rodrigues and Bowers, 1995). This becomes an especially significant issue when dealing with dynamic environments that require innovative and adaptative solutions.

The Standard seems to be obsessed with writing "treatment plans", as though the only allowable product of risk management is a specific separate document titled: "*The Treatment Plan*"[133]. Such an emphasis is in direct conflict with other parts of the Standard, especially the founding principle of "integration". How is encouraging separate treatment plans supposed to be 'integrated' into the rest of the organisation?

Resolution

Section 6.5 of the Standard should abandon the primary focus on 'treatment planning' (except where a standalone document may be justified) and instead be more focused on developing 'treatment strategies' or 'treatment solutions'. Activities that can then be more easily incorporated into the relevant organisational strategies and approaches, for example into existing or intended change management, business re-engineering, organisational improvement, new investments, mergers and acquisitions, and other projects and programs. Thus, allowing risk management to become properly integrated, or better still, embodied into the wider organisation.

Even if specific 'treatment planning' is deemed necessary, the Standard's approach is a very old fashioned view of what planning treatments should comprise, as well some major considerations that have been omitted:

[133] We occasionally come across auditors (usually from the big accounting firms) that make adverse findings because risk treatments were not recorded in a standalone document called a 'risk treatment plan'. Despite that risk treatment strategies were incorporated into ('integrated'!) into other documented activities of the organisation, and were being delivered as part of a larger managed changed project or program. This is one of the reasons why this separate treatment plan emphasis in the Standard has to change.

- The very start of planning treatment solutions should be to define the objectives for the treatment, if this is not understood at the start then the outcome will be highly uncertain.
- For a risk management Standard, it is very surprising that ISO 31000 does not mention the importance of understanding and addressing risk associated with the planning activities themselves, including designing and implementing risk treatments!
- There is no mention of aligning with current project planning and project governance frameworks that exist within the organisation.
- There is no consideration of shortening project development and implementation phases, or of regular end user review and acceptance as the project progress.
- There is no consideration of the use of rational expectancy prioritisation, such as using MoSCoW[134] planning throughout the treatment process.
- There is no consideration of the need for a methodology (and criteria) for evaluating the implementation of treatment effectiveness and efficiency, including post-project implementation reviews and benefits realisation evaluation. Note that evaluation is also often closely associated with monitoring.

[134] What **M**ust be done, What **S**hould be done, What **C**ould be done (if additional time and resources become available) or need to be postponed to the next iteration, what **W**on't be done during this iteration (Miranda, 2022).

The section on monitoring

In section 6.6, the Standard again misunderstands the overall purpose of monitoring and review, stating that it is to: "assure and improve the quality and effectiveness of process design, implementation and outcomes". Yes, this is *partly* true, one of the purposes is to monitor the conduct of the various risk management processes, but this heavy procedural focus is only a small element of monitor and review. Equally, perhaps even more importantly, monitoring should be undertaken to provide early warnings and insight into changes within the external and internal contexts, that may indicate the development of situations upon which the organisation (or stakeholders) must act. It is also important in ensuring that risk information remains current and relevant for decision-making, and that treatments are actually being put in place in a way that will achieve the required modification of risk, in the most effective and efficient manner.

Resolution

If risk management is truly embodied (or even "integrated') then monitoring should not be an isolated activity just occurring as part of the risk management process. High performing organisations have a range of monitoring, situational awareness, sensemaking and foresighting arrangements, and 'risk management monitoring' should be firmly incorporated into these other approaches (Gonzalez, 2022; McNamara, 2022; Vuorinen, 2022; WHO, 2022; OECD, 2015; Reynolds and Sutherland, 2013; Bezold, 2010; Popper, 2008; Ruff, 2006).

The section also misses the natural linkages to the organisation's mechanisms for lessons learned and for driving improvement.

The section on recording and reporting

Section 6.7 of the Standard is correct in emphasising the need for documenting and reporting, although in keeping with the rest of ISO 31000, the section is rather vague and lacks detailed guidance. Placing this section at the very end of the Standard, and its position within Figure 4 of the Standard reinforces the perception that this is the final stage of a linear process. Recording and reporting is not an end of risk management process activity, but should be occurring throughout the entire process and be embedded diagrammatically into each and every other 'box' in Figure 4 of the Standard. It would indeed be a strange process if some form of record (even if on a whiteboard during a risk workshop) was not made of the various outputs of risk assessment, evaluation, and treatment.

There is empirical evidence from many organisations' risk management processes, that the Standard's Figure 4 is reproduced without alteration and that reporting is slavishly conducted only at the end of the process. This was not the intention of the original approach upon which ISO 31000 was based[135].

Whilst reporting information should be occurring throughout the risk management process, reporting is also a key activity that would be a channel for communication and consultation. Again, this is not a relationship shown within the Standard

Given the previous comments, to a large extent we do agree with the list of dot pointed aims for recording and reporting presented in this section, although it should be noted that these aims are all *associated with communication and consultation*.

Resolution

The revision of ISO 31000 needs to address the current deficiencies in the section on reporting and recording, including:

- A close alignment and integration with 'monitoring and review'.
- Demonstrating interdependencies across the whole risk management process.
- Outlining the key concepts of recording and reporting, the types of data and information available, and how these can be used.
- An explanation of the key activities involved in recording and reporting, including:
    - developing objectives for reporting and recording;
    - scoping and planning recording and reporting activities;
    - developing activity planning for data & information identification, gathering, collation, validation, cleansing, alignment, coherency, reporting and presentation formats, audience requirements, frequency of reporting, distribution channels, privacy and confidentiality management, etc.

The current approach, having 'recording and reporting' as a separate section from 'monitoring' should also be reviewed, and consideration be given to developing them into a single more comprehensive section.

[135] The joint Australian and New Zealand Standard AS/NZS 4360:1995; 1999; 2004.

The other bits that are missing

As well as errors, misstatements, vagueness, and incompleteness prevalent within the text and diagrams of ISO 31000:2018, throughout the Standard, there are also has a number of omissions relating directly to what are substantial concepts in the management of risk.

Issue: what about the decision-maker?

The Standard mentions decision-making 18 times, each time referring to decisions, decision-making, and decision-makers as some nebulous thing happening somewhere (non-specific). The Standard fails to build the relationships between 'risk management' and vital concepts such as 'situational awareness' (never mentioned), 'sensemaking' (never mentioned), and decision-making (vaguely referred to).

At its simplest decision making will involve:

- Decisions about 'risk'.
- Decisions affected by 'risk'.
- Decisions informed by 'risk'.
- Decisions that ignore 'risk'.

In addition to the formal outputs of risk management that inform decision-making, even with the best available quantitative results, a decision maker will interpret risk-related results through filters based on their own independent situational awareness and understanding of risk (Aven, 2016b). Accordingly, risk management cannot be a 'black box' which spits out a risk rating with the expectation that decisions will be made solely relying on that value (a practice encompassed by some proponents of 'risk-based' decision making'). How decision-makers undertake their own independent separate assessment of risk (*risk-informed* decision making) is critically important, but is not addressed by ISO 31000.

Resolution

How decision-making and risk relate to each other needs to be explored in the next revision of the Standard. However, care needs to be taken to avoid the trap that some publications make, that risk management and decision-making are almost identical process. There is a whole science about decision-making and decision theory, that goes way beyond the field of risk management.

Issue: a perception of badness

ISO 31000's predecessor, AS/NZS 4360, was one of the earliest publications that challenged the popular understanding of 'risk' as something 'bad' that could happen[136], and instead introduced the concept that risk could also be accompanied by beneficial characteristics. Although ISO 31000 has continued the stance of 'neutrality' (that risk is associated with both positive and negative effects), the vast majority of practical applications of the Standard are overwhelmingly focused on 'negative risk', and struggle with including 'positive risk' in a meaningful way.

We chose deliberately to include the terms 'positive risk' and 'negative risk' above, firstly because they are very commonly used, and secondly because they are absolute nonsense, if one is to be consistent with the ethos of ISO 31000. Risk (as defined by the Standard) has no conceptualisation of either 'positive risk' or 'negative risk'. Risk is just… well risk, and a specific risk can be associated with a variety of consequences, some of which may be harmful and some that may be beneficial. Even to the extent that, for some individual risks, the consequences may be overwhelming harmful for one particular organisation, but for another organisation may have more equal trade-offs between harm and benefits.

This duality of risk-associated consequences can be problematic in risk assessment where only harmful consequences are considered, and where there may be 'hidden' beneficial consequences that could offset (at least partially) the value of negative consequences. Also, as we have discussed previously in this Whitepaper, 'opportunity' is neither the opposite of risk (or opposite of threat), or another word for a 'positive risk'. In fact, even speaking about 'risk and opportunity' together in this way displays a lack of understanding of the definition of risk as used in ISO 31000.

Resolution

It is apparent from the frequency with which practitioners and others talk about 'negative risk' and 'positive risk', and refer to opportunity as an 'opposite' of threat and risk, that the Standard has not provided sufficient guidance about the nature of risk. The revision of the Standard has to clearly establish that:

- There is neither positive or negative risk, this is a label of convenience used by some consultants, practitioners, and other stakeholders.
- Any risk could have both potential negative and positive effects (costs/losses and benefits), and how we view each risk should depend upon on how *we each* balance the likelihood and extent of success and failure.
- That an opportunity is a set of circumstances which we could use to achieve certain desirable future outcomes, and that in pursuing this 'opportunity' there is uncertainty about what benefit and harm may actually occur.

[136] An understanding that has persisted in the English speaking world since the mid-17th century.

Issue lack of consideration of risk governance

ISO 31000:2018 provides a very shallow consideration of the broader concept of governance, especially with regards to its interrelationships with risk management.

Similarly, the concept of 'risk governance' is not addressed by the Standard. Although there are a range of views about risk governance, the concept is well established in the literature[137] (Andersen et al, 2014; Corporate Governance Council, 2012; Wu and Saunders, 2011). In this respect, risk governance is regarded as one of the principal governance domains (aspects of corporate governance that receive a dedicated focus[138]) along with other domains such as sustainability, strategic alignment, assurance, human capital management, data and information, etc.

'Risk governance' is regarded as being part of the *accountability* of the 'governing body' (e.g., the Board), with 'risk management' (as a sub-component of risk governance) being the *responsibility* of the management.

Resolution

The structure, architecture, and composition of 'risk governance' would incorporate a revised concept of 'risk framework' (not achieved by the current Standard). Where 'risk management' comprises the process element of a much wider concept of risk governance and corporate governance, rather than the other way around. Such a revision would allow for the mobilisation of risk governance to be a major influence on the design and execution of the internal controls and other arrangements for understanding and managing risk within the established context.

Issue: is there a problem with maturity?

A number of commentators have raised the need for a future revision of the Standard to include some discussion of risk maturity and maturity frameworks. However, great caution is required for a Standard to include guidance about maturity models. Maturity models are used in a wide variety of different domains, and numerous organisations report their beliefs about their value. However, the evidence in support of the many different models is sparse. The use of risk maturity models in improving the effectiveness of risk management is even more dependent upon belief than evidential fact.

One of the key problems associated with risk management maturity models is that they are largely focussed on progressing towards an increasing range of different 'inputs' that are increasingly more involved and complex activities. This thinking promotes a maturity model that is focused more on 'doing stuff'[139] (input-focussed) that 'achieving stuff' (output and outcome-focussed).

A more 'mature' organisation should be one which is achieving more success in managing risk and making better decisions about uncertainty (and risk).

[137] Directing and controlling through the system of policies, rules, standards, codes, and practices.
[138] For example, Wu and Saunders, 2011.
[139] And may not even the most appropriate activities for the particular strategic or operating contexts.

Resolution

Including maturity models or frameworks into the Standard could be dangerous territory given the current lack of robust evidence for their use in risk management.

However, the revised Standard could provide guidance on the characteristics of effective and efficient risk management, and from which readers of the Standard could build their own outcome-based maturity models, should they wish to do so.

Issue: confused about where the framework ends and the process begins?

Other important aspects of the risk management framework that are only superficially considered in the Standard are:

- How does the framework interlink with other organisational systems and frameworks?
- What are meaningful measures of the effectiveness of the risk management framework?
- Under what circumstances should the framework be substituted for a different (even temporary) approach?
- In practical terms how the framework and risk management process actually interrelate?

It should also be noted that many of the components of the 'risk management process' should also be core components of the framework, such as communication and consultation, monitoring and review, recording and reporting, etc. There is still much confusion about how the risk framework and risk process work together in practice. The 'risk management framework', as a distinct entity, is a relatively new concept for the risk management approach.

The original standards (AS/NZS 4360: 1995, 1999, 2004) incorporated much of what we would now regard as 'framework' within the risk management process itself, and within the concept of the 'risk program'. When ISO 31000 introduced its framework section, the original 'framework' elements were also left intact within the risk management process. Resulting in some of the redundancies and confusion that we see today.

Resolution

There is a possibility to re-think what risk management means and what it could look like from both the framework and process perspectives. This leads us to an interesting proposition, could the risk management approach be fully reimagined to allow performance evaluation to occur within a broader risk framework and program (Figure 11). Leaving the process to focus on analysis and evaluation of risk and the generation of insight. Such an approach could then strengthen the framework as the driving force for risk management.

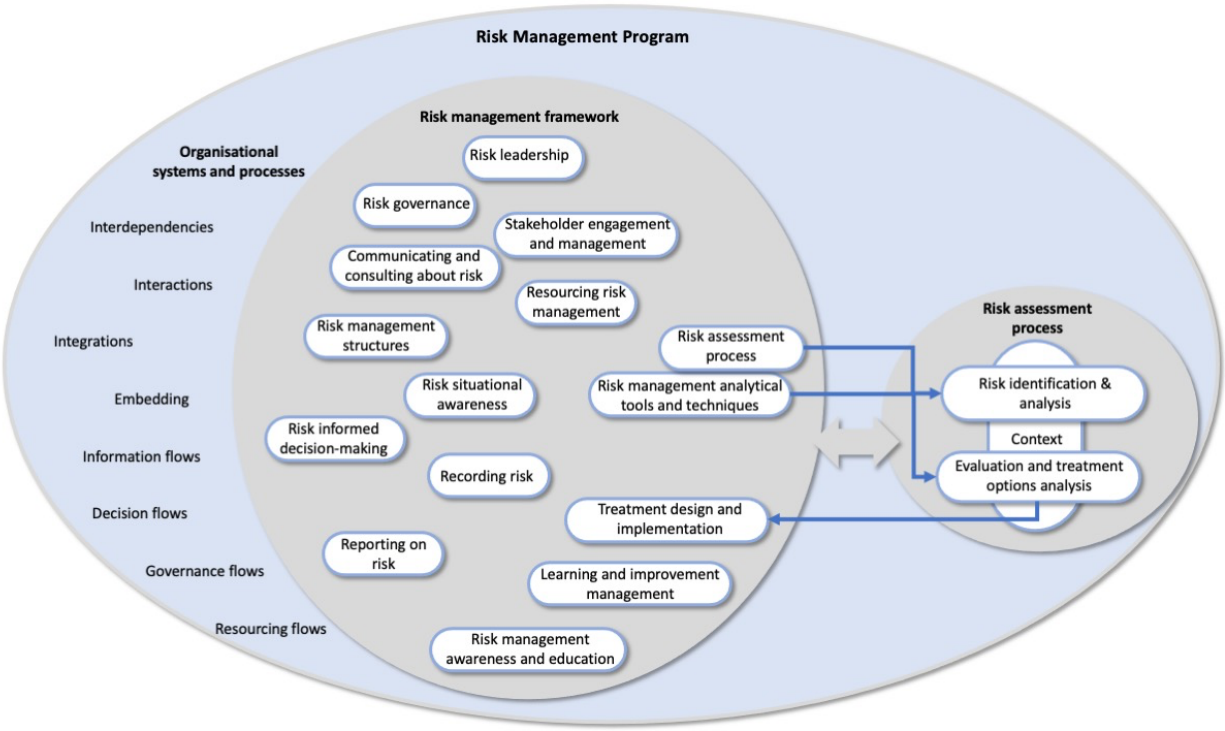


Figure 11: Risk management a reimagining[140]

Issue: data analytics, at least mention it

There have been a number of substantial developments since the publication of the Standard in 2018, including in the field of data analytics.

Resolution

As this field of interest increases in its application and importance, the next version of the Standard needs to include at least an overview of the role that data analytics is now playing in risk management (Nguyen et al, 2021; Ruia, 2021; Araz et al, 2020; Ivanov, 2019).

[140]Note that this is only illustrative, it is not meant to be comprehensive or provide a structural recommendation. It is merely a thought piece to spark conversation about reimaging the components of risk management.

Issue: what has happened to the concept of a risk management program?

The original risk management Standard (AS/NZS 4360: 1995[141]) provided an informative Appendix on establishing a risk management program, the concept of which is not considered in ISO 31000:2018. This should not be confused with a risk management framework, which ostensibly comprises the organisation's elements concerned with managing risk. A risk management program is much more expansive than a framework. A risk management program concerns the ways in which risk is addressed both strategically and operationally, whilst the framework comprises the artefacts by which the program is achieved.

Resolution

The revision of the Standard should consider providing guidance on the concept of a risk management programs and how a framework helps deliver that program.

[141] Standards Australia (1995).

In conclusion

There are significant numbers of practitioners that treat ISO 31000 as akin to 'holy writ', and in their belief they unthinkingly apply what is written within the Standard as 'gospel'. However, because much of the Standard is couched in terms of generalities and provides mostly only platitudinous guidance, the reader is left to make assumptions in order to interpret and apply the Standard. These assumptions are rarely consciously surfaced or acknowledged by practitioners, and are even more rarely challenged. We have lost count of the number of times that a practitioner (or auditor) has justified some concept or activity, by claiming "it is what the Standard says", with the claim then unable to be substantiated.

The near zealotry of some for only using the Standard 'as written' is only further reinforced by some senior management and Boards' mistaken insistence for 'conformance' with the Standard, and some audit firms' (and certification consultants') desire for 'compliance' with the Standard.

There is no arguing that thousands of practitioners across the world find ISO 31000:2018 to be useful. It is:

- Simple, so is easy to understand.
- Generic, so can be relevant to any organisation.
- Short in length, so the concepts can be quickly picked up and are easy to remember.
- Principles based, so does not get bogged down in complex analytics, or onerous management system standard's requirements.

This is probably why this Standard is the most successful and arguably the best Standard associated with risk management.

However, it is also arguably a poor standard because it is:

- Simplistic, so it lacks sufficient guidance, encourages misassumptions and misinterpretations, and does nothing to correct bad practices.
- Generic, so provides little beyond vague concepts, again requiring assumptions to made, and lacks enough detail to provide effective understanding,
- Short in length, so that the absolute desire of the responsible ISO committee to produce the shortest document possible, means a substantial amount of essential information has to be left out, thus further forcing the Standard to be overly simplistic.
- Principles based: conveying the assumption that the listed principles are the key principles on which risk management has to be based, although they most probably are not.

It is a common perception amongst many that all one has to do is read the fifteen key pages of the Standard, and then one can practice risk management. There quickly comes a realisation for these individuals, that there is far more to risk management than is contained within the Standard, and so they often seek training courses (and maybe also certification). However, many of these training courses are developed and run by individuals that have little understanding beyond what is contained within the Standard itself[142]. Even then, because of the vagueness of much of the Standard, these

[142] One of the authors of this Whitepaper has been previously asked to deliver already prepared training courses for a well-known and respected training organisation. To actually deliver the courses, up to 90% of the course content had to be replaced because the information was either out of date or incorrect.

course developers are adding in their own assumptions, are misinterpreting and misunderstanding the content of the Standard, and are failing to understand many key aspects of uncertainty and risk.

Subsequent to the publication of the latest version of the Standard by ISO in 2018, there was an intense debate amongst Australian and New Zealand experts as to whether ISO 31000:2018 should be adopted as a joint national standard. Many of the problems with ISO 31000 had been previously identified and communicated to the responsible ISO technical committee. However, it appears that Australia and New Zealand could not put forward a strong enough case, as many of the improvement recommendations were not included in the new version of the Standard. Because of these remaining problems, there were serious discussions about resurrecting and revising AS/NZ 4360 as the new Australian Standard for risk management. One counter argument held sway, that multinationals, and those organisations trading or working overseas did not want to have to deal with two different types of risk management Standard, especially if there were conceptual differences or conflicts between the two. Accordingly, the Standard was adopted as AS/NZS ISO 31000:2018. However, there was a proviso, that the issues with the Standard would be dealt with in a revision of the risk management handbook, HB 436. Work stared on a high level guide for Boards and senior executives and was published as a part 1 handbook. Then COVID-19 struck, the focus shifted to publishing the interim Standard on managing disruption-related risk (AS/NZS 5050(int):2020, following which the risk management committee (OB007) went into a de facto hibernation for much of the pandemic.

The authors' position is that ISO 31000:2018 is still (despite its many issues), probably still the best Standard out there. However, its issues are so manifest, that the Standard has to change dramatically if it is to remain relevant and useful. There are some that would argue that many of the issues we have raised in this Whitepaper should not be addressed in the body of the Standard itself, but in additional guidance material. We agree that ISO 31000 should focus largely on the 'what' aspect of risk management, and the highly detailed practical 'how' can be published separately. However, ISO 31000:2018 currently fails to fulfil its prime objectives. Whilst some of the matters that we have raised could indeed be more fully explored in other ISO publications, ISO 31000 has to be able to stand on its own in providing sufficient evidence based guidance.

The current Standard provides an acceptable foundation upon which a far better Standard can be built. However, this requires not just a 'revision', but a *complete reform* from the ground up. Over the last few years, we have been canvassing this idea and have received a somewhat mixed bag of responses. Overall, the idea of such a reform has been welcomed by the majority of practitioners that we have spoken with. They are aware of some (if not all) of the problems with ISO 31000:2018, and want to see them fixed. Then there are those practitioners that are relatively new to risk management, that are frustrated by the vagueness of ISO 31000, and do not find other ISO publications such as the "Practical Guide" published in 2021, or "ISO/IEC 31010: 2019 Risk management techniques", to be particularly useful[143]. These content and lack of guidance problems with ISO 31000 and associated Standards is perhaps why there is a plethora of books, journals and magazine articles, blogs, online videos, and training courses trying to explain what the Standard means and how to apply it. As with many practitioners, the developers of these additional guidance materials have had to make a range of assumptions about the Standard, and so we have even less consistency, and more myths and misunderstanding populating the risk management domain.

[143] In informal surveys conducted at training courses, conferences, webinars, and with clients, over 90% (of over 500 individuals) have either never heard of ISO/IEC 31010, or have made no attempt to use the Standard. One of the authors of this Whitepaper recently recommended ISO 31010 to a practitioner. They came back to the author, saying "I bought a copy, but it's really just a list of techniques, I want actual guidance on how these can be used in risk assessment"

On the other side, our stance on the reform of ISO 31000 has met some resistance, particularly from some practitioners, consultants, and software developers (not from all, some do recognise and agree with the need for reform). These individuals are concerned that any major change to ISO 31000 will invalidate what they have spent a lot of time, energy, and money establishing to sell to their customers. This will be one the challenges that any reform of ISO 31000 has to achieve, to bring to life a new Standard that does not immediately disenfranchise all of those that have made significant investment into risk management over many years. We all should not have to throw out what we already have in place, once a new 31000 is published. Instead, the new Standard should guide improvement to existing approaches and help to mature risk management knowledge and practice.

The 'bones' of ISO 31000:2018 are good enough to build upon and achieve this.

A final commentary

There are a number of myths about the development of ISO standards such as ISO 31000:

- *An ISO Standard is international best practice*. No, it is not. Many ISO Standards are written to be accessible and used in a wide range of countries with different levels of development, and in the case of ISO 31000 different levels of experience, knowledge and maturity in risk management. ISO 31000 is a *basic* level guideline. Many organisations and 'risk practitioners' that consider using the Standard are already well in advance of its guidance.

- *The content of the Standard is based upon the latest knowledge*. Some of it might be, but more often than not, the Standard includes content that has been circulating in the risk management domain for many years, and accordingly can be out of date. Many ISO Standards have differing levels of 'legitimacy' in their content, for example ISO 31000:2018 has a high content of conjecture, a moderate amount of content derived from individual experience, and a small amount of content that is supported by rigorous peer reviewed evidence.

- *The Standard is based upon solid evidence provided by international experts*. Although the membership of the relevant technical committees are called 'experts' they may be a very mixed bag. Whilst there may be some internationally acknowledged world leading experts involved, many are not, and are just dedicated individuals that want to contribute. A number of 'experts' are also self-appointed (through the mechanisms of their local standards bodies) rather than having to demonstrate their credentials. There will also be members that are not subject matter experts (e.g., experts in risk management) but are instead standardisation professionals (appointed because of their knowledge of the standards development processes).

- *The standard process of having so many different experts involved, and a commenting period guarantees a high quality peer review process*. Not necessarily, a small group of interested committee members will nominate themselves to be a member of a working group to develop a new Standard. Given that there could be 40 plus countries eligible to be involved on a working group, there are often only a small handful that actually do any development work. When the drafts are finally ready to be reviewed, the working group decides how to deal with any comments from member countries, and valid comments may be disregarded during the review. Decisions are made on a consensus basis, which involves the overall result of the balloting of individual experts or member country's Standardisation body (including those that may not have relevant expertise, or in some cases may not have even properly reviewed the document having the same voting rights as those that are deeply involved and deeply knowledgeable.

All of this means that there is a high variability in the quality of ISO Standards, and Australian mirror committees have on several occasions voted to not accept an ISO Standard for adoption into Australia.

References

ADB (2011). *Sensitivity and Risk Analysis*. Introductory Course on Economic Analysis of Investment Projects, Session 2.4, 5-9 July 2010. Asian Development Bank.

Agnese P. and Capuano P. (2020). *Risk Governance and Performance: Evidence form Eurozone's Large Banks*. International Journal of Financial Research 11(5) pp. 28-41.

Ahimbisibwe A., Daellenbach U. and Cavana R.Y. (2017). *Empirical Comparison of Traditional Plan-based and Agile Methodologies: Critical Success Factors for Outsourced Software Development Projects from Vendors' Perspective*. Journal of Enterprise Information Management 30(3) pp. 2017.

Alijoyo F.A. and Norimarna S. (2021). *The Role of Enterprise Risk Management (ERM) Using ISO 31000 for the Competitiveness of a Company That Adopts the Value Chain (VC) Model and Life Cycle Cost (LCC) Approach*. 3rd International Conference on Business, Management and Finance, 11 March 2021. Oxford United Kingdom.

Allen C.D. (2008). *Lessons Not Learned*. Armed Forces Journal September 2010, pp. 30-33.

Allington N.F.B., McCombie J.S.L., and Pike M.(2012). *Lessons Not Learnt: From the Collapse of the Long-term Capital Management to the Subprime Crisis*. Cambridge Centre for Economic and Public Policy CCEPP WP03-12, Department of Land Economy, University of Cambridge.

Allnutt M.F. (1987). *Human Factors in Accidents*. British Journal of Anaesthesia 59 pp. 856-864.

Alvesson M. and Sveningsson S. (2011). *Management is the Solution: Now What Was the Problem? On the Fragile Basis for Managerialism*. Scandinavian Journal of Management 27(4) pp. 349-361.

Alviniussen A. and Jankensgård H. (2018) *The Risk-Return Tradeoff: A Six-Step Guide to Ending the Curse of Risk Appetite*. Available at SSRN: https://ssrn.com/abstract=3174591 or http://dx.doi.org/10.2139/ssrn.3174591

Alviniussen A. and Jankensgård H. (2015). *Value and Risk: Enterprise Risk Management in Statoil*. In: Implementing Enterprise Risk Management: Case Studies and Best Practices. (Editors: J.R.S. Fraser, B.J. Simkins, and K. Narvaez), John Wiley & Sons, Hoboken, NJ.

Alviniussen A. and Jankensgård H. (2009). *Enterprise Risk Budgeting: Bringing Risk Management into the Financial Planning Process*. Journal of Applied Finance 19 pp. 178-192.

American Diabetes Association. (2019). *10. Cardiovascular Disease and Risk Management: Standards of Medical Care in Diabetes*. Diabetes Care 42(Suppl. 1): pp. S103–S123

Andersen T.J. and Young P.C. (2020). *Strategic Risk Leadership: Engaging a World of Risk, Uncertainty, and the Unknown*. Routledge, London.

Araz O.M., Choi T.-M., Olson D.L., and Salman F.S. (2020). Role of Analytics for Operational Risk Management in the Era of Big Data. Decision Sciences 51(6) pp. 1320-1346.

Arruda W. (2016). *9 Differences Between Being a Leader and a Manager*. Forbes 15 November, 2016. Accessed at:
https://www.forbes.com/sites/williamarruda/2016/11/15/9-differences-between-being-a-leader-and-a-manager/?sh=35db437c4609.

Ashgarian H., Krygier D., and Vilhelmsson A. (2022). *Systemic Risk and Centrality: The Role of Interactions.* European Financial Management 28 pp. 1199-1226.

Asobee M.S. (2021). *Exploring the Importance of Strategic Thinking to Strategic Planning in the Strategic Management Process*. Journal of Business and Management Sciences 2021, 9(2) pp. 68-70.

ASSNServices (2018). *Don't Attend the Old School of Strategic Planning*. World Class Boards, 25 April 2018.
Accessed at: https://www.worldclassboards.org/dont-attend-the-old-school-of-strategic-planning/.

Aven E. and Aven T. (2015). *On the Need for Rethinking Current Practice that Highlights Goal Achievement Risk in an Enterprise Context*. Risk Analysis, 35 pp. 1706-1716.

Aven T. (2015). *Implications for Black Swans to the Foundations and Practice of Risk Assessment and Management*. Reliability Engineering and Systems Safety 134 pp. 83-91.

Aven T. (2006). *On the Precautionary Principle, in the Context of Different Perspectives on Risk*. Risk Management 8(3). pp. 192-205.

Aven T. (2016a). *Implications of Black Swans to the Foundations and Practice of Risk Assessment and Management*. Reliability Engineering and System Safety 134 pp. 83-91.

Aven T. (2016b). *Supplementing Quantitative Risk Assessments with a Stage Addressing the Risk Understanding of the Decision Maker*. Reliability Engineering & System Safety 152 pp. 51-57.

Aven T. (2106c). *Risk Assessment and Risk Management: Review of Recent Advances on Their Foundation*. European Journal of Operational Research 253 pp. 1-13.

Aven T. (2017a). *The Flaws of ISO 31000 Conceptualisation of Risk*. Journal of Risk and Reliability 231(5) pp. 467-468.

Aven T. (2017b). *Improving Risk Characterisations in Practical Situations by Highlighting Knowledge Aspects, with Applications to Risk Matrices*. Reliability Engineering and System Safety 167 pp. 42-48.
Aven T. and Ylönen M. (2019). *The Strong Power of Standards in the Safety and Risk Fields: A Threat to Proper Developments of These Fields?* Reliability Engineering and System Safety 189 pp. 279-286.
Aven T. and Renn O. (2020). *Some Foundational Issues Related to Risk Governance and Different Types of Risks.* Journal of Risk Research 23 (9) pp. 1121-1134.
AXA (2019). *Future Risks Report 2019*. AXA and Eurasia Group.
Ayyub BM (2001) *Elicitation of Expert Opinions for Uncertainty and Risks*. CRC Press, Boca Raton.
Baer W.C. (2007). *General Plan Evaluation Criteria: An Approach to Making Better Plans*. Journal of the American Planning Association 63(3) pp. 329-344.
Bajec P., Tuljak-Suban D., and Krmac E. (2015). *Do ISO Standards Favour Logistics Provider Efficiency, Competitiveness and Sustainability? A Slovenian Perspective*. The International Journal of Logistics Management 26(2) pp. 275-295.
Balfe N. and Leva. M.C. (2014). *Human Factors Analysis in Risk Assessment*. In: Contemporary Ergonomics and Human Factors 2014, Proceedings of the International Conference on Ergonomics & Human Factors 7-10 April (Editor: S. Sharples and S.T. Shorrock), pp. 77-84. Southampton, UK.
Balog-Way D., McComas K., and Besley J. (2020). *The Evolving Field of Risk Communication*. Risk Analysis 40(S1) pp. 2240-2262.
Baur C. (2022). Opinion Piece; An Expert Opinion About the Problem with Expert Opinions. Research Square 23 October 2022. Accessed at: https://www.researchsquare.com/blog/issues-with-expert-opinions.
Baynes F.J. Lee I.K., and Stewart I.E. (2002). *A Study of the Accuracy and Precision of Some Landslide Risk Analyses*. Australia Geomechanics: News 37(2) pp. 149-155.
Beasley M.S., Branson B.C., and Hancock B.V. (2019). *The State of Risk Oversight 2019: An Overview of Risk Management Practices. Enterprise Risk Management Initiative*. AICPA and Poole College of Management: Risk Management Initiative, 10th Edition. North Carolina State University, NC. Accessed at: https://erm.ncsu.edu/az/erm/i/chan/library/2019_Current_Report_on_State_of_Risk_Oversight.pdf.
Bergman B. and Klefsjö B. (2003). *Quality*. 2nd ed Studentlitteratur Lund, Sweden.
Berry A. and Phillips J. (1998). *Enterprise Risk Management: Pulling it Together*. *Risk Management*, vol. 45(9) 98 Article 5.
Bertsimas D. and Thiele A. (2006). *Robust and Data-Driven Optimization: Modern Decision Making Under Uncertainty*. Tutorials in Operations Research, Informs 2006pp. 95-12.
Bezold C. (2010). *Lessons from Using Scenarios for Strategic Foresight*. Technological Forecasting and Social Change 77 pp. 15-13-1518.
Bilgin B. and Brenner L. (2013). *Context Affects the Interpretation of Low but Not High Numerical Probabilities: A Hypothesis Testing Account of Subjective Probability*. Organizational Behavior and Human Decision Processes 121(8) pp. 118-128.
Biodiversa (2014). *Stakeholder Engagement Handbook*. Bioiversa, Paris, France.
Birkland T.A. (2009). *Disasters. Lessons Learned, and Fantasy Documents*. Journal of Contingencies and Crisis Management 17(3). pp. 146-156.
Bland A.R. and Schaeffer A. (2012). *Different Varieties of Uncertainty in Human Decision-making*. Frontiers in Human Neuroscience 6 Article 85.
Blockley D. (2009). *Uncertainty, Prediction, or Control*. International Journal of Engineering Under Uncertainty, Hazards Assessment and Mitigation 1(1-2) pp. 73-80.
Blockley D. (2013). *Analysing Uncertainties: Towards Comparing Bayesian and Interval Probabilities*. Mechanical Systems and Signal Processing 37 pp. 30-42.
Blum D. (2020). *Case Study: How FAIR Risk Quantification Enables Information Security Decisions at Swisscom*. Accessed at:
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/how-fair-risk-quantification-enables
Bond S. and Cooper S. (2006). *Modelling Emergency Decisions: Recognition-primed Decision Making. The Literature in Relation to an Ophthalmic Critical Incident*. Journal of Clinical Nursing 15(8) pp. 1023-32.
Booker J.M. and Ross T.J. (2011). *An Evolution of Uncertainty Assessment and Quantification*. Scientia Iranica, Transactions D: Computer Science & Engineering and Electrical Engineering 18(3) pp. 669-676.
Boon S. (2022). *What is Treasury Risk Management? Risk Types, Strategies & Solutions*. Nomentia, 16 December 2022. Accessed at:

https://www.nomentia.com/blog/treasury-risk-management#:~:text=This%20typically%20includes%20activities%20such,financial%20positions%20are%20accurately%20reported.
Borgelt K and Falk I. (2008). *The Leadership/management Conundrum: Innovation or Risk Management?* Leadership and Organisational Development Journal 28(2) pp. 122-136.
Borgert C.J., Sargent E.V., Vasella G., Dietrich D.R., McCarty L.S., and Golden R.J. (2012). *The Human Relevant Potency Threshold: Reducing Uncertainty by Human Calibration of Cumulative Risk Assessments*. Regulatory Toxicology and Pharmacology 62(2) pp. 313-328.
Bouhali R., Mekdad Y., Lebsir H., and Ferkha L. (2015). *Leader Roles for Innovation: Strategic Thinking and Planning*. 3rd International Conference on Leadership, Technology and Innovation Management. Procedia – Social and Behavioral Sciences 181 pp. 72-78.
Boyce S. (2013). *Follow the Framework.* The Treasurer, October 2013.
Brewer L.E., Wright J.M., Rice G., Neas L., and Teuschler L. 92017). *Causal Inference in Cumulative Risk Assessment: The Roles of Directed Acyclic Graphs*. Environment International 102 pp. 30-41.
Browne E.C. and Brüne M. (2012). *The Role of Prediction in Social Neuroscience*. Frontiers in Human Neuroscience 6 Article 147.
Brugnach M., Dewulf A., and Henriksen H.J., van der Keur P. (2010). *More is Not Always Better: Coping with Ambiguity in Natural Resources Management*. Journal of Environmental Management.
Burgman M.A., McBride M., Ashton R., Speirs-Bridge A., Flander L. Wintle B., Rumpff L. and Twardy C. (2011) *Expert Status and Performance*. PLoS ONE 6(7): e22998.
Burgoon J.K., Wang R.X., Chen X., Ge T.S. and Dorn B. (2022). *How the Brunswikian Lens Model Illustrates the Relationship Between Physiological and Behavioral Signals and Psychological Emotional and Cognitive States*. Frontiers in Psychology 12 Article 781487.
Burnham G. (2016**).** *Is Management by Objectives Misunderstood?* Accessed at: https://www.linkedin.com/pulse/management-objectives-misunderstood-gregory-burnham/
Busman E.R. (1998). *The Challenge Ahead: Adopting an Enterprise-wide Approach to Risk*. Risk Management 45(1) Article 3.
Calder B.R. and Schwehr K (2009). *Traffic Analysis for the Calibration of Risk Assessment Methods*. U.S. Hydrographic Conference. 451.
Cantu J., Tolk J., Fritts S., and Gharehyakheh A. (2020). *High Reliability Organization (HRO) Systematic Literature Review: Discovery of Culture as a Foundational Hallmark*. Journal of Contingencies and Crisis Management. 28(4) pp. 399-410.
Cardona P. and Rey C. (2022). *The Limits of Management By Objectives*. In Management by Mission, Chapter 3 pp. 35-48. Palgrave Macmillan, Springer, Cham, Switzerland.
Cartwright S. (2002). *Double-Loop Learning: A Concept and Process for Leadership Educators*. Journal of Leadership Education 1(1) pp. 68 -71.
Casadesús M. and Karapetrovic S. (2005a). *The Erosion of ISO 9000 Benefits: A Temporal Study*. International Journal of Quality and Reliability Management 22(2) pp. 120-36.
Casadesús M. and Karapetrovic S. (2005b). *An Empirical Study of the Benefits and Costs of ISO 9001:2000 Compared to ISO 9001/2/3: 1994*. Total Quality Management 16 (1) pp. 105-20.
Casey B. (2019). *Failing Fast, Traditional Strategy, and How They Work Together*. IBM, 4 October 2019. Accessed at: https://www.ibm.com/cloud/blog/failing-fast-traditional-strategy-and-how-they-work-together.
CFI Team (2023). *Importance of Risk Management in Finance*. Corporate Finance Institute. Accessed at: https://corporatefinanceinstitute.com/resources/risk-management/importance-of-risk-management-in-finance/.
Chapelle A. (2016). *The Missing Piece of in Operational Risk Appetite*. Risk Net, 12 September 2016. Accessed at: https://www.risk.net/risk-management/2470332/the-missing-piece-in-operational-risk-appetite.
Charness N. and Tuffiash M. (2008). *The Role of Expertise Research and Human Factors in Capturing, Explaining, and Producing Superior Performance*. Human Factors 50(3) pp. 427-432.
Chassin M.R. and Loeb J.M. (2013). *High-reliability Health Care: Getting There from Here*. Milbank Quarterly 91(3) pp. 459-490.
Chi M.T.H. (2006) *Two Approaches to the Study of Experts' Characteristics*. In: The Cambridge Handbook of Expertise and Expert Performance. (Editors; K.A. Ericsson, N. Charness, P.J. Feltovitch, R.R. Hoffman) pp. 21–30. Cambridge University Press, Cambridge UK.
Christianson M.K., Sutcliffe K.M., Miller M.A. and Iwashyna T.J. (2011). *Becoming a High Reliability Organisation*. Critical Care 15, Article 314.

Chuilá H. and Uribe J.M. (2019). *Expected, Unexpected Good and Bad Uncertainty*. Working Paper 2019/19. Research Institute of Applied Economics, University of Barcelona, Spain.
Clark D.L. (1981). *In Consideration of Goal-Free Planning: The Failure of Traditional Planning Systems in Education*. *Educational Administration Quarterly 17*(3) pp. 42–60.
Coate J. (2020). *COVID 19 Hotel Quarantine Inquiry Final Report and Recommendations, Volume 1*. December 2020. Parliamentary Paper No 191 (2018-2020), Melbourne Australia.
Coles E. (2014). *Learning the Lessons from Major Incidents: A Short Review of the Literature*. Emergency Planning College Occasional Papers, New Series Number 10.
Coleman H.W. (2020). *The Improvement Paradox: The Trouble with Small Incremental Improvements*. Channel Connection, 11 September, 2020. Accessed at: https://channelconnection.nbmda.org/Full-Article/the-improvement-paradox-the-trouble-with-small-incremental-improvements.
Communitynet (2013). *Governance and Management*. Communitynet Aotearoa, 25 July, 2013. Accessed at: https://community.net.nz/resources/community-resource-kit/4-2-governance-governance-and-management/#:~:text=Governance%20is%20the%20job%20of,his%2Fher%20staff%20and%20volunteers.
Connors M.H. and Large M.M. (2023). *Calibrating Violence Risk Assessments for Uncertainty*. General Psychiatry 36(2) Article e100921.
Cornelius M. (2023). *A Comprehensive Guide to the Dynamic Risk Assessment*. Safety Culture, 19 May 2023. Accessed at: https://safetyculture.com/topics/dynamic-risk-assessment/.
Corporate Governance Council (2012). *Risk Governance Guidance for Listed Boards*. 10 May 2012, Singapore.
COSO (2017). *Enterprise Risk Management – Integrating Strategy and Performance*. Committee of Organizations of the Treadway Commission.
Cox L.A. (2008). *What's Wrong With Risk Matrices*? Risk Analysis 28(2) pp. 497-512.
Covello V.T., von Winterfeldt D., and Slovic P. (1988). *Risk Communication*. In Carcinogen Risk Assessment. Contemporary Issues in Risk Analysis, vol 3: (Editor: C.C. Travis). Springer, Boston MA.
Croskerry P. (2014). *ED Cognition: Any Decision by Anyone at Any Time*. Canadian Journal of Emergency Medicine 16(1) pp. 13-9.
Cunliffe A.L. (2016). *"On Becoming a Critically Reflexive Practitioner" Redux: What Does It Mean to Be Reflexive?* Journal of Management Education 40(6) pp, 740-746.
Damgaard C., Holmstrup M., Schmidt I.K., Beier C., and Larsen K.S. (2018). *On the Problems of Using Linear Models in Ecological Manipulation Experiments: Lessons Learned from a Climate Experiment*. Ecosphere https://doi.org/10.1002/ecs2.2322.
De Bruyckere V. (2015). *Systemic Risk Rankings and Network Centrality in the European Banking Sector. Working Paper Series*. European Bank, Fellowship Program, No 1848, September 2015.
Dekker S.W.A. (2013). *Drifting into Failure: Complexity Theory and the Management of Risk*. In: Chaos and Complexity Theory for management: Nonlinear Dynamics, pp. 241-253, (Editor: Banerjee S.). Hershey, PA.
Dekker S. (2015). *Safety Differently: Human Factors for a New Era*. CRC Press, London, New York.
Deming W. E. (2000). *The New Economics*. MIT CAES, 2nd ed Cambridge, MA.
Dewulf A. and Biesbroek R. (2018). *Nine Lives of Uncertainty in Decision-making: Strategies for Dealing with Uncertainty in Environmental Governance*. Policy and Society 37(4) pp. 441-458.
Dhami M.K. and Mumpower J.L. (2023). *Kenneth R. Hammond's Contributions to the Study of Judgment and Decision making*. Cambridge Core, 1 January 2023. Cambridge University Press.
Dick G.P.M., Heras I., and Casadesús M. (2008). *Shedding Light on Causation Between ISO 9001 and Improved Business Performance*. International Journal of Operations and Production Management 28(7) p.p. 687-708.
Dickson G. (1995). *Principles of Risk Management*. Quality in Health Care 4 pp. 75-79.
Dickinson G. (2001). *Enterprise Risk Management: Its Origin and Conceptual Foundation*. The Geneva Papers on Risk and Insurance 26(3) pp. 360-366.
Diderich C. (2020). *Design Thinking for Strategy: Innovating Towards Competitive Advantage*. Management for Professional Series. Springer Nature, Switzerland.
Dinesh D. and Palmer E. (1998). *Management by Objectives and the Balanced Scorecard: Will Rome Fall Again?* Management Decision 36(6) pp. 363-369.
Di Russo S. (2016). *Understanding the Behaviour of Design Thinking in Complex Environments*. Thesis, Swinburne University of Technology, Melbourne.
Dörmer D. and Funke J. (2017). *Complex Problem Solving: What it is and What it is Not*. Frontiers in Psychology 8 1153.
Dosi G. and Egidi M. (1991). *Substantive and Procedural Uncertainty*. Journal of Evolutionary Economics 1 pp. 145-168.

Dos Santos R.B., Lima F.G., Gatsios R.C., de Almeida R.B. (2017). *Risk Management and Value Creation: New Evidence for Brazilian Non-financial Companies*. Applied Economics 49 (58) pp. 5815-5827.
Emblemsvåg J. and Endre Kjølstad L. (2006). *Qualitative Analysis: Some Problems and Remedies*. Management Decision 44(3) pp. 395-408.
Dwyer J., Karanikas N., and Sav A. (2023). *Scoping Review of Peer-reviewed Empirical Studies on Implementing High Reliability Organisation Theory*. Safety Science 164, Article 106178.
EMV (2021). *Dynamic Risk Assessment. Joint Standard Operating Procedure, J08.02*. Emergency Management Victoria, 17 September 2021. Accessed at: https://files-em.em.vic.gov.au/public/JSOP/SOP-J08.02.pdf.
EPA (2021). *Follow a Risk Management Process*. Environment Protection Authority Victoria. Accessed at: https://www.epa.vic.gov.au/for-business/how-to/manage-environmental-risk/risk-management-process.
Epstein I. (2009). *Promoting Harmony where there is Commonly Conflict: Evidence-informed Practice as an Integrative Strategy*. Social Work in Health Care, 48, 216–231.
Epstein (2011). *Reconciling Evidence-based practice, Evidence-informed practice, and Practice-based Research: The Role of Clinical Data Mining*. Social Work, 2011(56), 284–288.
Fan Y. and Stevenson M. (2018) *A Review of Supply Chain Risk Management: Definition, Theory, and Research Agenda*. International Journal of Physical Distribution and Logistics Management, 48(3) pp. 205-230.
Fairholm M.R. and Card M. (2009). *Perspectives of Strategic Thinking: From Controlling Chaos to Embracing it*. Journal of Management and Organization 15 pp. 17-30.
Figueroa P. (2016). *Nuclear Risk Governance in Japan and the Fukushima Triple Disaster: Lessons Unlearned*. In: Disaster Governance in Japan and the Fuskushima Triple Disaster: Lessons Unlearned, (Editors M.A. Miller and M .Douglass), Springer, Singapore.
Flouris T. and Ylmaz A.Y. (2010). *The Risk Management Framework to Strategic Human Resource Management*. International Research Journal of Finance and Economics 36 pp. 25-45.
Feng M., Terziovski M., and Samson D. (2007). *Relationship of ISO 9001:2000 Quality System Certification with Operational and Business Performance: A Survey in Australia and New Zealand-based Manufacturing and Service Companies*. Journal of Manufacturing Technology Management 19(1) pp. 22-37.
Fischer P., Fischer J., Weisweiler S., and Frey D. (2010). *Selective Exposure to Information: How Different Modes of Decision Making Affect Subsequent Confirmatory Information Processing*. British Journal of Psychology 49 pp. 871-881.
Fischhoff B, Slovic P., and Lichtenstein S. (1982). *Lay Foibles and Expert Fables in Judgements About Risk*. American Statistician 36: 240–255.
FM Global (2010) *The Risk/Earnings Ratio: New Perspectives for Achieving Bottom-Line Stability*. Published with Oxford Metrica. FM Global, Johnston RI, USA. Accessed at:
http://oxfordmetrica.com/public/CMS/Files/1716/02_FMGlobal.pdf
Franceschini F., Galetto M., Mastrogiacomo L. and Viticchie L. (2008). *Diffusion of ISO 9000 and ISO 14000 Certification in Italian Commodity Sectors.* International Journal of Quality and Reliability Management 25(5) pp. 452-64.
Franceschini F., Galetto M., Maisano D., and Mastrogiacomo L. (2010). *Clustering of European Countries Based on ISO 9000 Certification Diffusion*. International Journal of Quality and Reliability Management 27(5) pp. 558-575.
Franceschini F., Galetto M., and Mastrogiacomo L. (2018). *ISO 9001 Certification and Failure Risk: Any Relationship*. Total Quality Management 29(11) pp. 1279-1293.
Fraser J.R. (2015). Simkins B.J., and Narvaez K. (2015). *Implementing Enterprise Risk Management: Case Studies and Best Practices*. Wiley & Sons, Hoboken NJ.
Fraser J.R.S. (2014). *Building Enterprise Risk Management into Agency Processes and Culture*. In: Managing Risk and Performance: A Guide for Government Decision Makers. (Editors T. Stanton and D.W. Webster), John Wiley & Sons, Hoboken, NJ.
Friedrich T.L. and Mumford M.D. (2009). *The Effects of Conflicting Information on Creative Thought: A Source of Performance Improvements or Decrements*. Creativity Research Journal 12(2-3) pp. 265-281.
Funabashi Y. and Kitazawa K. (2012). *Fuskushima in Review: A Complex Disaster, a Disastrous Response.* Bulletin of the Atomic Scientists 68(2). Accessed at: http://thebulletin.org/2012/march/fukushima-review-complex-disaster-disastrous-response.
Furlan A., Grandinetti R., and de Toni A.F. (2023). *Managing the Lean-Agile Paradox in Complex Environments*. Systems 11(5) Article 258.

Galetto M., Franceschini F., and Mastrogiacomo L. (2017). *ISO 9001 Certification and Corporate Performance of Italian Companies***.** International Journal of Quality and Reliability Management 34(2) pp. 231-250.
Gavin M. (2019). *Leadership vs. Management: What's the Difference*? Harvard Business School Online, 31 October 2019. Accessed at: https://online.hbs.edu/blog/post/leadership-vs-management.
Gandz J. and Seijts G. (2013). *Leadership and Risk Culture*. Ivey Business Journal, March/April 2013
Gentry J.W. (1990). *What is Experiential Learning?* In: Guide to Business Gaming and Experiential Learning, Chapter 2. Nichols Publishing, Asbury IA.
Ghicajanu M. (2008). *Strategic Planning and Control in Management by Objectives*. Annals of the Oradea Uiversity, Fascicle of Management and Technological Engineering Volume VII (XVII), 2008.
Giarini O. (2011). *Science and Economics: The Case of Uncertainty & Disequilibrium*. Cadmus 1(2) pp. 25-34.
Gerstein D.M., Kallimani J.G., Mayer L.A., Meshkat L., Osburg J., Davis P., Cignarella B., and Grammich C.A. (2016). *Developing a Risk Assessment Methodology for the National Aeronautics and Space Administration*. Rand Corporation, Santa Monica, California.
Gibson C.A. (2020). *Perspectives on Resilience*. Monograph. Accessed at:
https://www.arpi.org.au/media/mongraphs-in-risk-and-resilience.
Gibson C.A. and Gibson K. (2023a). *Incident Investigation and lessons Learned*. In: A Critical Incident Field Guide: Integrating Risk, Business Continuity, Emergency, and Crisis Management. Volume 1 Concepts.
Gibson C.A. and Gibson K. (2023b). *Incident Investigation and lessons Learned*. In: A Critical Incident Field Guide: Integrating Risk, Business Continuity, Emergency, and Crisis Management. Volume 2 Application.
Gifford A. (2013). *Risk Appetite: Cut Through the Hype.* In: Managing Business Risk A Practical Guide to Protecting Your Business pp. 11-23, (Edited: J. Reuvid). Kogan Page, London.
Gladwell M. (2005). *Blink: The Power of Thinking Without Thinking*. Back Bay Books, New York, NY.
Godlock G.C., Miltner R.S., and Sullivan D.T**.** (2017). *Deference to Expertise: Masking Care Safer.* Creative Nursing 23(1) pp. 7-12.
Gold Standard (2019). *Gold Standard for the Global Goals: Stakeholder Consultation and Engagement Guidelines*. October 2019, Gold Standard Foundation.
Gonzalez A. (2022). *Strategic Environmental Assessment Monitoring: The Enduring Forgotten Sibling*. Impact Assessment and Project Appraisal 40(2) pp.168-176.
Goodchild E. (1998) *The Business Benefits of EMS Approaches*. PhD Thesis, University of Salford, UK.
Good Governance Institute (2021). *Management or Governance?* 28 July 2021. Accessed at: https://www.good-governance.org.uk/publications/insights/management-or-governance
GO-Science (2012). *Blackett Review of High Impact Low Probability Risks.* Government Office for Science, 13 January 2012.
Gotzamani K.D. and Tsiotras G.D. (2001*). An Empirical Study of the ISO 9000 Standards' Contribution Towards Total Quality Management*. International Journal of Operations & Production Management 21 (10) pp. 1326–1342.
Govindarajan D. (2011). *Corporate Risk Appetite: Ensuring Board and Senior Management Accountability for Risk*. ICMA Centre Discussion Papers in Finance DP2011-22.University of Reading, UK.
Grable J. (2020). *Uncovering Inconsistency in Financial Risk Assessment*. University of Georgia.
Graf S. (2021). *Design Thinking for Strategizing? – A Critical Literature Review*. Journal of Emerging Trends in Marketing and Management – 1(1) pp. 110-119.
Gutteling J.M. and Wiegman (1996). *Exploring Risk Communication*. Springer Science and Business Media. Cham, Switzerland.
Halbesleben J.R.B., and Buckley M.R. (2004). *Burnout in Organizational Life*. Journal of Management 30(6) pp. 859-879.
Halvorson S.J. and Hamilton J.P. (2010). *In the Aftermath of the Qa'yamat: the Kashmir Earthquake Disaster in Northern Pakistan*. Disasters 34(1) pp. 184-204.
Han P.K.J., Klein W.M.P., and Arora N.J. (2011). *Varieties of Uncertainty in Health Care: A Conceptual Taxonomy.* Medical Decision Making 31(6) pp. 828-838.
Hand D.J. (2020). *Dark Data: Why What You Don't Know Matters*. Princeton University Press, Princeton NJ.
Hanson J.M. (2015). *The Admiralty Code: A Cognitive Tool for Self-Directed Learning*. International Journal of Learning, Teaching and Educational Research 14(1) pp. 97-115.
Hardy C. and Maguire S. (2016). *Organizing Risk: Discourse, Power and Riskification*. Academy of Management Review 41(1) pp. 80–108.
Hart S.O. and Cooke D.J. (2013). *Another Look at the (Im-)Precision of Individual Risk Estimates Made Using Actuarial Risk Assessment Instruments*. Behavioral Sciences and the Law 37 (1) pp. 81-102.

Head B.W. (2014). *Evidence, Uncertainty, and Wicked Problems in Climate Change Decision Making In Australia*. Environment and Planning C: Politics and Space 32(4) pp. 663-679.
Head B. and Alford J. (2008). *Wicked Problems: The Implications for Public Management*. Panel on Public Management in Practice. International Research Society for Public Management, 12th Annual Conference, 26-28 March, 2008, Brisbane Australia.
Heracleous L. (1998). *Strategic Thinking or Strategic Planning?* Strategy at the Leading Edge: New Research & Conference Reports pp. 481-487.
Heath R.L. and O'Hair H.D. (2010). *The Significance of Crisis and risk Communication*. Taylor and Francis, London UK.
Henriksen K., Dayton E., Keyes M.A., Carayon P., and Hughes R. (2008). *Chapter 5: Understanding Adverse Events: A Human Factors Framework*. In: Patient Safety and Quality: An Evidence Based Handbook for Nurses (Editor: R.G. Hughes). Agency for Healthcare Research and Quality, Rockville, MD.
Heras-Saizatbitoria I., Boiral O., and Allur E. (2018). *Three Decades of Dissemination of ISO9001 and Two of 14001: Looking Back and Ahead.* In: ISO9001, ISO14001, and New Management System Standards pp. 1-16, (Editor: I. Heras-Saizatbitoria), Springer, Cham, Switzerland.
Henriques V. and Tanner M. (2017). *A Systematic Literature Review of Agile and Maturity Model Research*. Interdisciplinary Journal of Information, Knowledge, and Management 12 pp. 53-73.
Hertin J., Berhout F., Wagner M., and Tyteca D. (2008). *Are EMS Environmental Effective. The Link Between Environmental Management Systems and Environmental Performance in European Companies*. Journal of Environmental Planning and management 52 pp. 259-283.
Hillson D. (2015). *Weight Loss for Risky Projects*. Project Management Institute, Newton Square PA.
Hochrainer-Stigler S., Šakić R.T., Reiter K., Ward P.J., de Ruiter M.C., Duncan M., Torresan S., Ciurean R., Mysiak J., Stuparu D., and Gottardo S. (2023). Toward a Framework for Systemic Multi-hazard and Multi-risk Assessment and Management. iScience 26 Article 106736.
Holberton D., McAndre D., and Simpson C. (2019). *What Makes a Successful Risk Leader*. Risk Management, RIMS, 1 April 2019.
Holmes C.E. (2011). *Queensland Floods Commission of Inquiry – Interim Report*.
Holmes C.E. (2012). *Queensland Floods Commission of Inquiry – Final Report.*
Howe L. Johnston S., and Côte C. (2023). *Mining-related Environmental Disasters: A High Reliability Organisation (HRO) Perspective*. Journal of Cleaner Production 417, Article 137965.
Hubbard (2014). *How to Measure Anything. Finding the Value of 'Intangibles' in Business*. Wiley, Hoboken, NJ.
Hubbard D.W. (2020). *The Failure of Risk Management: Why its Broken and How to Fix it*. Wiley, New York, NY.
Hubbard D.W. and Seiersen R. (2017). *How to Measure Anything in Cybersecurity Risk*. Wiley, New York, NY.
Hussin W.N.W., Bamahros H.M., and Shukeri S.N. (2018). *Lead Engagement Partner Workload, Partner-Client Tenure and Audit Reporting Lag: Evidence from Malaysia*. Managerial Auditing Journal 33(3) pp. 246-266.
Inanoglu H. and Jacobs M. (2009). *Models for Risk Aggregation and Sensitivity Analysis: An Application to Bank Economic Capital*. Journal of Risk and Financial Management 2 pp. 118-189.
IFC (2007). *Stakeholder Engagement: A Good Practice Handbook for Companies Doing Business in Emerging Markets.* International Finance Corporation, World Bank Group, Washington DC.
IHI Team (2021). *How to Build a Learning Organisation Culture*. Institute for Healthcare Improvement, 20 July, 2021. Accessed at: https://www.ihi.org/communities/blogs/how-to-build-a-whole-system-quality-learning-organization-culture.
IIA (2023). *Control Assessment: A Framework*. Whitepaper, Institute of Internal Auditors Australia. Accessed at: https://www.iia.org.au/sf_docs/default-source/technical-resources/iia-whitepaper_control-assessment-a-framework.pdf.
Inegbedion H., Inegbedion E., Peter A., and Harry.L. (2020). *Perception of Workload Balance and Employee Job Satisfaction in Work Organisations*. Heliyon 6 Article e03160.
Infrastructure Australia (2021). *Guide to Risk and Uncertainty Analysis*. Technical Guide of the Assessment Framework. July 2021, Australian Government.
Inghels D. (2020). *Systems Thinking and Introduction to System Dynamics Modeling*. In: Introduction to Modeling Sustainable Development in Business Processes pp. 141-147. Springer, Cham.
Isler O., Yilmaz O., and Dogruyol B. (2020). *Activating Reflective Thinking with Decision Justification and Debiasing Training*. Judgement and Decision Making 15(6) pp. 926-938.
Ittner C.D., and Keusch T. (2016). *Incorporating Risk Considerations into Planning and Control Systems: The Influence of Risk Management Value Creation Objectives*. In: The Routledge Companion to Accounting and Risk (Editors: Philip Linsley and Margaret Woods). Routledge, London.

Ivanov D., Dolgui A., Das A., and Sokolov B. (2019). *Digital Supply Chain Twins: Managing the Ripple Effect, Resilience and Disruption Risks by Data-driven Optimization, Simulation, and Visibility*. In: Handbook of Ripple Effects in the Supply Chain (Editors: D. Ivanov, A. Dolgui, and B. Sokolov), International Series in Operations Research & Management Science Vol 276. Springer, Cham, Switzerland.
Jackson S.E., May K.E., and Whitney K. (1995). *Understanding the Dynamics of Diversity in Decision-Making Teams*. In: Team Effectiveness and Decision Making in Organizations, pp. 204-261. Jossey-Bass, San Francisco, CA.
Jacowitz K.E. and Kahneman D. (1995). *Measures of Anchoring in Estimation Tasks*. Personality and Social Psychology Bulletin 21 pp. 1161-1166.
Jafari M., Rezaeenour J., Mazadeh M.M., and Hooshmandi A. (2011). *Development and Evaluation of a Knowledge Risk Management Model for Project-based Organizations: A Multi-stage Study*. Management Decision 49(3) pp. 309-329.
Jamieson B.D. (1973). *Behavioural Problems with Management by Objectives*. Academy of Management Journal 16(3) pp. 496-505
Jankensgård H. (2019). *A Theory of Enterprise Risk Management*. Corporate Governance: The International Journal of Business in Society 19(3) pp. 565-579.
Jarvis W.F. (2014). *Assessing Your Board's Risk Tolerance: Establishing and Understanding the Risk Tolerance of an Organization's Investment Leadership Body are Critical to Avoid Investment Losses that can Negatively Impact the Mission of the Organization*. Healthcare Financial Management 68(1) pp. 141
Joint investigation (2016). *Joint Investigation of Ashely Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner and Acting Australian Information Commissioner*. Government of Canada and Australian Government.
Jorion P. (2007). *Value at Risk: The New Benchmark for Managing Financial Risk*. 3rd Edition. McGraw Hill , Boston MA.
Kafel P. and Simon A. (2017). *The Reasons for Decertification of ISO9001: Financial Aspects*. Quality, Innovation, Prosperity Journal 21(3) pp. 173-184.
Kanchu T., and Kumar M.M. (2013). *Risk Management in Banking Sector -An Empirical Study*. International Journal of Marketing, Financial Services, and Management Research 2(2) pp. 145-153.
Kahneman D. (2003). *A Perspective on Judgment and Choice: Mapping Bounded Rationality*. American Psychologist 58(9) 697-720.
Kahneman D. (2011). *Thinking, Fast and Slow*. Farrar, Straus and Giroux. New York, NY.
Kahneman D., Slovic P., Lichtenstein S. (1982). *Judgement Under Uncertainty: Heuristics and Biases*. Cambridge University Press, Cambridge UK.
Kahneman D. and Tversky A. (1979). *Prospect Theory: An Analysis of Decisions Under Risk*. Econometrica 47 pp. 313-327.
Kamensky J.M. (2011). *Managing the Complicated vs. The Complex*. Business of Government, Fall/Winter 2011 pp. 66-70.
Kaplan L. Farooque M., Sarewitz D., and Tomblin D. (2021). *Designing Participatory Technology Assessments: A Reflexive Method for Advancing the Public Role in Science Policy Decision-making*. Technological Forecasting and Social Change. 171 Article 120974.
Kaplan R.S. (2010). *Conceptual Foundations of the Balanced Scorecard*. Working Paper 10-074, Harvard Business School.
Karabacak B. and Sogukpinar I. (2004). *A Novel Approach to Information Security Risk Analysis*. The 3rd Asia Pacific International Symposium on Information Technology.
Kardes F.R. (2006). *When Should Consumers and Managers Trust their Intuition?* Journal of Consumer Psychology 16 pp. 20–24.
Kernchen R. (2020). *Risk Forecasting in the Light of Big Data*. Journal of Risk Analysis and Crisis Response 10(4) pp. 160-167.
Klein G. (2008). *Naturalistic Decision Making*. Human Factors 50(3) pp. 456-460.
Klein G. (2015). *A Naturalistic Decision Making Perspective on Studying Intuitive Decision Making*. Journal of Applied Research in Memory and Cognition 4(3) pp. 164-168.
Klein G. (2022). *Innovation vs. Incremental Improvement*. Interaction Design Foundation. Accessed at: https://www.interaction-design.org/literature/article/innovation-vs-incremental-improvement.
Klein G., Jalaeian M., Hoffman R., and Mueller S.T. (2023). *The Plausibility Model of Sensemaking*. Frontiers in Psychology 14 Article 1160132.

Klein *G.A., Orasanu J.M., Calderwood R., and Zsambok C. (1993). Decision Making in Action: Models and Methods. Ablex Publishing, New York, NY,*
Kleynhans T.E. and Spies P.H. (1994) *The influence of Newtonian-Cartesian Scientific Thinking on the Interpretation of Welfare and Development.* Development Southern Africa 11(1) pp. 49-67.
Klikauer T. (2013). *Managerialism a Critique of an Ideology*. Palgrave Macmillan, Basingstoke, UK.
Klinker A. and Renn O. (2002). *A New Approach to Risk Evaluation and Management: Risk-based, Precaution-based, and Discourse-based strategies*. Risk Analysis 22(6) pp. 1071-1094.
Klinker A. and Renn O. (2011). *Precautionary Principle and Discursive Strategies: Classifying and Managing Risks*. Journal of Risk Research 4(2) pp. 150-173.
Knaub Z. (2017). *Organizational Agility; Winning in Today's Complex Environment*. The Strategy Bridge, 21 April 2017.
Knight E., Daymond J., and Paroutis S. (2020). *Design-Led Strategy: How To Bring Design Thinking Into The Art of Strategic Management*. California Management Review 62(2) pp. 30-52.
Kocken T. (2022). *Broadening our Thinking as the Basis for Finance Professionals: Dawn of the Complexity Paradigm*. VBA Journal 150 (Summer/Autumn) pp. 36-43.
Kochenderfer M.J., Amato C., Chowdary G., How J.P., Davison Reynolds J.J., Thornton J.R., Torres-Carrasquillo P.A., Üre N.K., and Vian J. (2015). *Decision Making Under Uncertainty: Theory and Application*. The MIT Press, Cambridge MA and London UK.
Kolb D.D. (1984). *Experiential Learning: Experience as the Source of Learning and Development*. Prentice Hall, Englewood Cliffs, NJ.
Kotterman J. 2006). *Leadership versus Management: What's the Difference?* The Journal of Quality and Participation 29(2) pp. 13-17.
Kraus V. and Lehner O.M. (2012). *The Nexus of Enterprise Risk Management and Value Creation: A Systematic Literature Review*. In: Proceedings in Finance and Risk Perspectives`12 ACRN Cambridge Publishing House.
Kric, T., Forstater M., Monaghan P., and Sillanpää M. (2005). *The Stakeholder Engagement Manual, vol. 2: The Practitioner's Handbook on Stakeholder Engagement***.** United Nations Environment Programme.
Kristamuljana A., Van Loon B., Bolt J., and Terblanché A. (2018). *Dynamic Risk Assessment*. Compact 2018, Smart Tech.
Krut R., and Gleckman H. (1998). *ISO 14001: A Missed Opportunity for Global Sustainable Industrial Development*. Earthscan, London, UK
Kumah E.A., McSherry R., Bettany-Saltikov J. Hamiltom J., Whittaker V., and van Schiak P. (2019). *PROTOCOL: Evidence-informed Practice Versus Evidence-based Practice Educational Interventions for Improving Knowledge, Attitudes, Understanding, and Behavior Toward the Application of Evidence into Practice: A Comprehensive Systematic Review of Undergraduate Students.* Campbell Systematic Reviews 15 Article e1015.
Kunreuther H. (2002). *Risk Analysis and Risk Management in an Uncertain World*. Risk Analysis 22(4) pp. 655-664.
Kwon H. and Kang C.W. (2019). *Improving Budget Estimation Accuracy and Precision by Analyzing Reserves for Both Identified and Unidentified Risks*. Project Management Journal 50(1) pp. 86-100.
Kyriakopoulos G. (2012). *Half a Century of Management by Objectives (MB): A Review*. African Journal of Business Management 6(5) pp. 1772-1786.
Lalond C. and Boiral O. (2012). *Managing Risks Through ISO 31000: A Critical Analysis*. Risk Management 14(4) pp. 272–300.
Landry L. (2020). What is Human Centred Design. Harvard Business School Insights 15 December 2020. Accessed at: https://online.hbs.edu/blog/post/what-is-human-centered-design.
Laquana R. (2022). *Management PDCA – Hero or Villain?* Accessed at: https://www.linkedin.com/pulse/management-pdca-hero-zero-raimund-laqua-pmp-peng/.
Larsen B. and Häversjö T. (2001). *Management by Standards – Real Benefits from Fashion.* Scandinavian Journal of Management 17(4) pp. 457-480.
Lee P.-L., Lye C.-T. and Lee C. (2022). *Is Bank Risk Appetite Relevant to Bank default in Times of Covid-19?* Central Bank Review 22 pp. 109-117.
Lees A., Meyer E., and Rafferty J. (2011). *From Menzies Lyth to Munro: The Problem of Managerialism*. British Journal of Social Work 43(3) pp. 542-558.
Leitch M. (2012). *The Risk Listing School*. Working in Uncertainty. Accessed at: http://www.workinginuncertainty.co.uk/risk_listing.shtml.
Leitch M. (2016). *The Fundamental Flaws of "ISO 31000: 2009 Risk Management – Principles and Guidelines"*. Working in Uncertainty. Accessed at: http://www.workinginuncertainty.co.uk/isoriskstandard.shtml

Lengyel D.M., Mazzuchi T.A., and Vesely W.E. (2023). *Establishing Risk Matrix Standard Criteria for use in the Continuous Risk Management Process*. Journal of Space Safety Engineering, https://doi.org/10.1016/j.jsse.2023.05.001.
Leo M., Sharma S., and Maddulety K. (2019). *Machine Learning in Banking Risk Management: A Literature Review*. Risks 7 Article 29.
Levinsohn A. (1098). *A Generation of Risk Managers Foretell a Future*. ABA Banking Journal 90(10) pp. 74-80.
Lewis C.M. and Mody A. (1097). *The Management of Contingent Liabilities. A Risk Management Framework for National Governments*. In: Dealing with Public Risk in Private Infrastructure (Editors: T. Irwin and others). World Bank Latin American and Caribbean Studies, Washington, D.C.
Lewis L. (2022). *The Difference Between Business Process Reengineering and Continuous Improvement*. ProcessMaker, 23 February, 2022. Accessed at: https://www.processmaker.com/blog/the-difference-between-business-process-reengineering-and-continuous-improvement/.
Li J., Hu Y., Zhou W. (2023). *Dynamic Risk Assessment of Emergency Evacuation in Large Public Buildings: A Case Study*. International Journal of Risk Reduction 91 Article 103659.
Lilly C.M., Cucchi E., Marshall N., and Katz A. (2019). *Battling Intensivist Burnout: A Role for Workload Management*. Chest 156(5) pp. 1001-1007.
Lines D. (2021). *Feedback loops are a prerequisite for Continuous Improvement*. SD Times, 12 July, 2021.
Lipshitz R. and Strauss O. (1997). *Coping with Uncertainty: A Naturalistic Decision-making Analysis*. Organizational Behavior and Human Decision Processes 69(2) pp. 149–163.
Liu B. (2011). *Why is There. a Need for Uncertainty Theory?* Journal of Uncertain Systems 6(1) pp. 3-10.
Lo C.K.Y., Yeung A.C.L., and Cheng T.C.E. (2011). *Meta-standards, Financial Performance and Senior Executive Compensation in China: An Institutional Perspective*. International Journal of Production Economics 129(1) pp. 119-126.
Lončar M. (2017). *The Impact of Strategic Management and Strategic Thinking Approaches on Business Performance of Companies Operating In the Retail Industry*. European Project Management Journal 7(1) pp. 85-98.
Longbine D.F. (2008). *Red Teaming Past and Present*. Monograph, School of Advanced Military Studies, Fort Leavenworth KS.
Lopes de Paula L.D.F., de Souza Silva L.C., Nobre F.C., and Nobre L.H.N. (2022). *Risk Tolerance Assessment in real Assets Investments: A Scale Validation in Brazil*. Rev. Adm. Santa Maria 15(2) pp. 257-269.
Lumen (2023). *Managerialism and Decision Making*. Lumen: Organisational Behaviour and Human Relations. Accessed at: https://courses.lumenlearning.com/wm-organizationalbehavior/chapter/managerialism-and-decision-making/#:~:text=The%20definition%20of%20managerialism%20is,and%20their%20needs%20and%20wishes.
Lundgren R.E. and McMakin A.H. (2018). *Risk Communication: A Handbook for Communicating Environmental, Safety, and Health Risks*. IEEE Press, Wiley, Hoboken NJ.
McLees T. (2023). *Navigating the Shift from Complicated to Complex Problem Solving*. Accessed at: https://medium.com/human-skills-project/navigating-the-shift-from-complicated-to-complex-problem-solving-808ddb4b69e7
McClory S., Read M., and Labib A. (2017). *Conceptualising the Lessons-Learned Process in Project Management: Towards a Triple-loop Learning Framework*. International Journal of Project Management 35(7) pp. 1322-1335.
McCarthy N., Neville K., Pope A., Gallagher A., Nussbaumer A., and Steiner C.M. (2016). *The Creation of a Training Model to Support Decision-making of Emergency Management Practitioners: A Design Research Study*. Journal of Decision Systems 25(1) pp. 558-565.
McGill E., Marks D., Er V., Penney T., Petticrew M., and Egan M. (2020). *Qualitative Process Evaluation from a Complex Systems Perspective: A Systematic Review and Framework for Public Health Evaluators*. PLOS Medicine 17(11) Article e 1003368
McHugh K. (2021). *Why You Should Know About Risk Leadership*. A Political, 27 May 2021. Accessed at: https://apolitical.co/solution-articles/en/why-you-should-know-about-risk-leadership.
McKinnell J. (2020b). *Cruise Ships Regularly Flouted NSW Government's Coronavirus Advice, Ruby Princess Inquiry Hears*. ABC News 17 June 2020, accessed on 3 August at: https://www.abc.net.au/news/2020-06-17/ruby-princess-inquiry-told-not- unusual-for-no-covid-swabs/12364182.
McMillan C. and Overall J. (2016). *Wicked Problems: Turning Strategic Management Upside Down*. Journal of Business Strategy 37(1) pp. 34-43.
MacNamara C. (2022). *Basics of Monitoring, Evaluating and Deviating from the Strategic Plan*. In: Field Guide to Nonprofit Strategic Planning and Facilitation, 4th Edition.

Madrigal J. (2011). *Research Brief: Incremental Innovation and Continuous Improvement*: Are They Related? Sustainable Innovation Management, 26 February, 2011.
Magd H. and Nabulsi F. (2012). *The Effectiveness of ISO 9000 in an Emerging Market as a Business Process Management Tool: the Case of the UAE*. Procedia Economics and Finance 3 pp. 158 – 165
Maglio S.J. and Polman E. (2016). *Revising Probability Estimates: Why Increasing Likelihood Means Increasing Impact*. Journal of Personality and Social Psychology 111(2) pp. 141-158.
Majola K. (2021) Risk Leadership: A Critical Adhesive to Risk Culture. PRIMA Intelligent Risk, February 2021. Accessed at:
https://issuu.com/prmia/docs/intelligent_risk-feb_2021-issuu/s/11701383#:~:text=Risk%20leadership%20is%20the%20anchor,and%20the%20Chief%20Risk%20Officer
Makinen G. (2002). *The Economic Effects of 9/11: A Retrospective Assessment. Report for Congress,* September 27, 2002. Accessed on 3 April 2017 at: http://www.dtic.mil/dtic/tr/fulltext/u2/a469198.pdf.
unusual-for-no-covid-swabs/12364182.
Malish R.G. and Sargent P.D. (2019). *High-Reliability Uncaged: Safety Lessons From Army Aviation*. Military Medicine 184(3/4) pp. 78-80.
Manolescu G. (2011). *Appetite For Risk Of The Bank (I)*". Studii Financiare (Financial Studies), Centre of Financial and Monetary Research "Victor Slavescu", 15(2) pp. 209-223.
Mark M.M., Henry G.T., and Julnes G. (1999). *Toward an Integrative Framework for Evaluation Practice*. 20(2) pp. 177-198.
Marle F and Vidal L-A. (2016). *Limits of Traditional Project Management Approaches When Facing Complexity*. In: Managing Complex, High Risk Projects, Chapter 2. Springer Link.
Márquez C.P. and Márquez A.D. (2020). *Whitepaper # V: Criticality Analysis Methods (Based on the Risk Assessment Process).* Technical Series: Reliability, Maintenance and Asset Management. Ingecon.
Marshall A. and Ojiako U. (2013). *Managing Risk Through a Veil of Ignorance*. Journal of Risk Research 16(10) pp. 1225-1239.
Marshall A., Udechukwu O., and Chipulu M. (2019). A Futility, Perversity and Jeopardy Critique of "Risk Appetite". International Journal of Organisational Analysis. 27(1) pp. 51-73.
Martens F. and Rittenberg L. (2020). *Risk Appetite – Critical to Success*. The Committee of Sponsoring Organizations of the Treadway Commission (COSO).
Marušić M.F., Fidahić M., Cepeha C.M., Farcaș L.G., Tseke A. and Puljak L. Marušić M.F., Fidahić M., Cepeha, C.M., Farcaș L.G., Tseke A. and Puljak L. (2020*). Methodological Tools and Sensitivity Analysis for Assessing Quality or Risk of Bias Used in Systematic Reviews Published in the High-impact Anesthesiology Journals*. BMC Medical Research Methodology 20 Article 21.
Matta N. and Ashkenas R. (2003). *Why Good Projects Fail Anyway*. Harvard Business Review, September 2003. Accessed at: https://hbr.org/2003/09/why-good-projects-fail-anyway.
Maze T. (2018). *Qualitative vs, Quantitative Analysis for Cyber Risk: What's the Difference?* Fair Institute. Accessed at: https://www.fairinstitute.org/blog/qualitative-vs.-quantitative-analysis-for-cyber-risk-whats-the-difference
Mear R. and Firth M. (1988). *Risk Perceptions of Financial Analysts and the Use of Market and Accounting Data*. Accounting and Business Research 18(72) pp. 335-340
Mercier H., and Landemore H. (2012). *Reasoning Is for Arguing: Understanding the Successes and Failures of Deliberation*. Political Psychology 33(2) pp. 243-258.
Messnarz R., O'Suilleabhain G., and Coughlan R. (2006). *From Process Improvement to Learning Organisations.* Software Process Improvement and Practice 11 pp. 287-294.
Meyer T. and Reniers G. (2022). *Engineering Risk Management, 3rd Edition*. De Gruyter Group Publishing.
Miranda E. (2022). *Moscow Rules: A Quantitative Exposé*. In: Agile Processes in Software Engineering and Extreme Programming. International Conference on Agile Software Development, XP 2022 Proceedings (Editors: V. Stray, K-J. Stol, M. Paasivaara, P. Kruchten), June 13-17 June 2022. Copenhagen, Denmark,
Moen R. and Norman C. (2009). *Evolution of the PDCA cycle*. In: Proceedings of the 7th ANQ Congress, 17 September 2009, Tokyo, Japan.
Morgan M.G. (2014). *Use and Abuse of Expert Elicitation in Support of Decision Making for Public Policy*. PNAS 111(20) pp. 7176-7184.
Mohanty S. (2020). *Risk Velocity and Dynamic Risk Assessment*. Global Risk Management Institute.
Morina R. (1994). *Discussion of When Numbers are Better than Words: The Joint Effects of Response Representation and Experience on Inherent Risk Judgments*. Sarasota 13: 24.
Morris T.H. (2019). *Experiential Learning – A systematic Review and Revision of Kolb's Model*. Interactive Learning Environments, Taylor and Francis Group.

Mun J. (2014). *A Primer on Quantitative Risk Analysis*. In: Multi Asset Risk Modeling: Techniques for a Global Economy in an Electronic and Algorithmic Trading Era. (Editors: M. Glantz and R. Kissell), Chapter 3. Academic Press Oxford, UK.
Muralikrishna I.V., and Manikam V. (2017). *Chapter 8 – Environmental Risk Assessment*. In: Environmental Management: Science and Engineering for Industry pp. 135-152. ScienceDirect, Elsevier Inc.
Nayer V. (2013). *Three Differences Between Managers and Leaders*. Harvard Business Review 2 August 2013.
Neal-Boylan L. and Rotkoff S. (2021). *Why Red Teaming is a Better Way*. In: Innovative Decision Making in Healthcare. Springer, Cham.
Nguyen T., Gosine R.G., and Warrian P. (2020). *A Systematic Review of Big Data Analytics for Oil and Gas Industry 4.0*. IEEE Access 8, pp. 61183-61201.
Petria N., Trenca I., and Mutus S. (2012). *The Tolerance and Operational Risk Appetite in Banking*. Revista Economica Supplement 4/2012 pp. 618-624.
NOPSEMA (2021). *Human Factors*. NOPSEMA, accessed at: https://www.nopsema.gov.au/offshore-industry/safety/human-factors.
Noroozi A., Khakzad N., Khan F., MacKinnon S., and Abbassi R. (2013). *The Role of Human Error in Risk Analysis: Application to Pre- and Post-maintenance Procedures of Process Facilities*. Reliability Engineering and System Safety 119 pp. 251-258.
Notebaert L., Masschelein S., Wright B., MacLeod C. (2021). *To Risk or Not to Risk: Anxiety and the Calibration Between risk Perception and Danger Mitigation*. Journal of Experimental Psychology, Learning, Memory and Cognition 42(6) pp. 985-95.
Noveck S. (2021). *Theories of Managerialism*. Political Science 1 October 2021, Yale University Press. Accessed at: https://yalebooks.yale.edu/2021/10/01/theories-of-managerialism/.
Nuntamanop P., Kauranen I., Igel B. (2013). *A New Model of Strategic Thinking Competency*. Journal of Strategy and Management 6(3) pp. 242-264.
O'Mara S. (2017). *The Importance of Cognitive Biases*. In: A Brain for Business – A Brain for Life. The Neuroscience of Business, pp. 61-65. Palgrave Macmillan, Cham.
OECD (2015*). Monitoring and Evaluating the Strategic Plan of Nuevo León 2015-2030: Using Evidence to Achieve Sustainable Development*. OECD, United Nations.
OECD (2019). *Better Evaluation Revised Evaluation Criteria Definitions and Principles for Use OECD/DAC Network on Development Evaluation*. OECD/DAC Network on Development Evaluation, November 2019.
Orros G., Badal V., Burke J.M., Byrne C.M., Chacko F., Garner M., Kaye P. and Noel D. (2011). *Risk Appetite for a General Insurance Undertaking*. Risk Appetite Working Party (GIRO).
Ostrom L. and Wilhelmsen C. (2019). *Basic Fault Analysis Technique*. In: Risk Assessment: Tools, Techniques and Their Applications. Wiley.
Osundahunsi A. (2012). *Effective Project Risk Management Using the Concept of Risk Velocity, Agility, and Resiliency*. Paper presented at PMI® Research and Education Conference, Limerick, Munster, Ireland. Newtown Square, PA: Project Management Institute.
Palmer J. (2011). *Risk Governance in an Age of Wicked Problems: Lessons from the European Approach to Indirect Land-Use Change*. Journal of Risk Research 15(5) pp. 495-513.
Parhizkar T., Utne I.B., and Vinnem J.-E. (2022). *Dynamic Risk Assessment to Assist Decision-Making in Emergency Situations.* In Online Probabilistic Risk Assessment of Complex Marine Systems pp. 17-39, Springer Series in Reliability Engineering, Springer.
Parker M. (2002). *Against Management: Organisation in the Age of Managerialism*. Wiley, London, UK.
Paulsen C., Boyens J., Bartol N., and Winkler K. (2018). *Criticality Analysis Process Model:" Prioritising Systems and Components*. US Department of Commerce, April 2018, NISTIR 8179.
Pearl J. and Mackenzie (2019). *The Book of Why. The New Science of Cause and Effect*. Penguin Random House, London.
Peeters L.J.M., Holland K.L., Huddleston-Holmes C., and Boulton A.J. (2022). *A Spatial Causal Network Approach for Multi-stressor Risk Analysis and Mapping for Environmental Impact Assessments*. Science of the Total Environment 802 Article 149845.
Peiries S. (2022). *Design Processes: More Than Just Linear*. Accessed at: https://shavinpeiries.com/non-linear-design/.
Platt M.L. and Huettel S.A. (2008). *Risky Business: The Neuroeconomics of Decision Making Under Uncertainty*. Nature Neuroscience 11(4) pp. 398-403.
Poksinska B. (2010). *When Does ISO 9000 Lead to Improvements?* International Journal of Productivity and Quality Management 5(2) pp. 124-136.

Poksinska B, Dahlgaard JJ, and Eklund JAE. (2003) *Implementing ISO 14000 in Sweden: Motives, Benefits and Comparisons with ISO 9000*. The International Journal of Quality and Reliability Management 20 pp. 585-606.
Polaski S. Carpenter S.R., Folke C., and Keeler B. (2011). *Decision-making Under Great Uncertainty: Environmental Management in an Era of Global Change*. Trends in Ecology and Evolution 26(8). Pp. 398-404.
Popper R. *How are Foresight Methods Selected*? Foresight 10(6) pp. 62-89.
Power M. (2009). The Risk Management of Nothing. Accounting, Organizations and Society 34 pp. 849-855.
Pozniak E. (2011). *Concept of Dynamic Risk Assessment: Does it Apply Everywhere?* American Society of Safety Professionals, Safety Conference, 2011 session no 673. Accessed at:
https://aeasseincludes.assp.org/proceedings/2011/docs/673.pdf
Pratt J.W. (1964). *Risk Aversion in the Small and in the Large*. Econometrica 32(1/2) pp. 122-136.
Pressman D.E. and Flockton J. (2012). *Calibrating Risk for Violent Political Extremists and Terrorists: The VERA 2 Structured Assessment*. The British Journal of Forensic Practice 14(4) pp. 237-251.
Prince2 (2018). *Risk Management Approach*. Prince2 Wiki. Accessed at: https://prince2.wiki/management-products/risk-management-approach/.
Proctor P. (2020). *Lesson Unlearned: The Army's Role in Creating the Forever Wars in Afghanistan and Iraq*. University of Missouri Press, Columbia, MO.
PSNET (2019). *Human Factors Engineering*. Patient Safety Network.
Accessed at: https://psnet.ahrq.gov/primer/human-factors-engineering.
Quail R. (2012). Defining Your Taste for Risk. Corporate Risk Canada, Spring 2012, pp. 25-30.
Quan N.S. and Chiang A. (2017). *Risk Management at the Speed of Business*. Directors Bulletin, 2017 Q1 pp. 24-27. PWC.
Rabin M. and Thaler R.H. (2001). *Anomalies: Risk Aversion*. Journal of Economic Perspectives 15(1) pp. 219-232**.**
Ramamoorti S. and Stover R. (2018). *Risk Consumption: Understanding the Difference between Risk Appetite and Risk tolerance can Deter Organizations from Digesting too Much Risk*. Internal Auditor 75(2) pp. 36.
Rampini G.H.S., Takia H., and Berssaneti F.T. (2019). *Critical Success Factors of Risk Management with the Advent of ISO 31000 2018 - Descriptive and Content Analyzes*. 25th International Conference on Production Research Manufacturing Innovation: Cyber Physical Manufacturing August 9-14, 2019 Chicago, Illinois.
Rausand M. and Hoyland A. (2004). *Systems Reliability Theory : Models, Statistical Methods, and Applications*. Wiley, Hoboken NJ.
Reason J. (1995). *Understanding Adverse Events: Human Factors*. Quality in Health Care 4 pp .80-89.
Recklies D. (2015). *Strategy Making in the Past and Today – Part 2: Problems with the Traditional Strategy Process*. The Manager.org., 25 August, 2015. Accessed at: https://www.themanager.org/2015/08/strategy-making-2-problems-traditional-strategy-process/.
Reed J.E. and Card A.J. (2015). *The Problem with the Plan-Do-Study-Act Cycles*. BMJ Quality and Safety 25 pp. 147-152.
Renn O. (2010). *Risk Communication: Insights and Requirements for Designing Successful Communication Programs on Health and Environmental Hazards*. In: Handbook of Risk and Crisis Communication (Editor O.Renn). Routledge.
Renn O. (2008). *Risk Governance: Coping with Uncertainty in a Complex World*. Earthscan.
Renn O. (2014). *Emerging Risks: Methodology, Classification and Policy Implications*. Journal of Risk Analysis and Crisis Response 4(3) pp. 114-132.
Renn O. (2020). *New Challenges for Risk Analysis: Systemic Risks*. Journal of Risk Research 24 pp. 127-13.
Renn O. (2004). *The Precautionary Principle: A New Paradigm for Risk Management and Participation*. Ideés Pour le Débat, No 03/2004, Enterprises et Biens Public. Institute du Développement et des Relations Internationales.
Reynolds H.W. and Sutherland E.G. (2013). *A Systematic Approach to the Planning, Implementation, Monitoring, and Evaluation of Integrated Health Services*. BMC Health Services Research 13 Article 168.
Robinson F.E., Shalin V.L., Steele-Johnson D., and Springer B. (2022. *Context Matter in Expert Performance*. Journal of Expertise 5(2-3) pp. 72- 104.
Rodrigues A. and Bowers J. (1995). *System Dynamics in Project Management: A Comparative Analysis with Traditional Methods*. System Dynamics Review 12(2) pp. 121-139.
Rohrmann B. (1992). *The Evaluation of Risk Communication Effectiveness*. Acta Psychologica 81(2) pp. 169-192.
Romme A.G.L. and van Witteloostuijn A. (1999). *Circular Organizing and Triple Loop Learning*. Journal of Organizational Change 12(5) pp. 439-453.

Rondinelli D. and Vastag G. (2000). *Panacea, Common Sense, or Just a Label? The value of ISO 14001 Environmental Management Systems*. European Management Journal 18(5) pp. 499-510.
Roseke B. (2022). *Guide to the Risk Management Process*. Project Engineer, 18 May 2022. Accessed at: https://www.projectengineer.net/guide-to-the-risk-management-process/.
Rozell D.J. (2015). *A Cautionary Note on Qualitative Risk Ranking of Homeland Security Threats*. Homeland Security Affairs 11 Article 3.
Roter A. B. (2017). *Understanding and Recognizing Dysfunctional Leadership: The Impact of Dysfunctional Leadership on Organizations and Followers*. Routledge London and New York.
Rotteau L., Goldman J., Shojania K.G., Vogus T.J., Christianson M., Baker G.R., Rowland P., and Coffey M. (2022). *Striving for High Reliability in Healthcare: A Qualitative Study of the Implementation of a Hospital Safety Programme*. BMJ Quality and Safety 31 pp. 867-877.
Rosqvist T., Havlik D., and Meriste M. (2017). *A Reference Decision Model of First Responders; Decision-Making*. International Journal of Emergency Management 13(3) pp. 193-209.
Ruia V. (2021). *Role of Data Analytics in Risk Management.* EY, 22 February 2021. Accessed at: https://www.ey.com/en_in/risk/role-of-data-analytics-in-risk-management.
Rycroft-Malone J. (2018). *From Linear to Complicated to Complex*. International Journal of Policy Development 7(6) pp. 566-568.
Safe Work Australia (2022). *Managing Risks*. Accessed at: https://www.safeworkaustralia.gov.au/safety-topic/managing-health-and-safety/identify-assess-and-control-hazards/managing-risks
Sainsbury R.M. (2009). *Paradoxes*. 3rd Edition, Cambridge University Press, Cambridge, UK.
Salas E., Maurino D., Curtis M., (2010). *Human Factors in Aviation: An Overview*. In: Human Factors in Aviation, 2nd edition. Elsevier Inc.
Salih A.A. and Alnaji L. (2014). *Impact of Strategic Thinking and Strategic Agility on Strategic Performance: A Case Study of Jordanian Insurance Industry Companies*. International Review of Management and Business Research 3(4) pp.1871-1882.
Saltelli A., Campolongo, and Saisana M. (2002). *Sensitivity Analysis for Risk Assessment*. Sixth International Conference on Probabilistic Safety Assessment and Management, 23-28 June 2002, Puerto Rico, USA.
San Cristóbal J.R., Carral L., Diaz E., Fraguela J.A., and Iglesias G. (2018). *Complexity and Project Management: A General Overview*. Complexity 2018, Article 4891286.
Sanders J.D. (2016). *Defining Terms: Data, Information and Knowledge*. SAI Computing Conference, 13-15 July 2016, London, UK.
Sandoz J.F. (2001). *Red Teaming: Shaping the Transformation Process: Annotated Briefing*. Joint Advanced Warfighting Program. Institute for Defence Analysis Alexandria VA.
Saunders R.P., Evans M.H., and Joshi P. (2005). *Developing a Process-Evaluation Plan for Assessing Health promotion Program Implementation: A How to Guide*. Health Promotion Practice 6(2) pp. 134-147.
Schein E.H. (1983). *Organisational Culture: A Dynamic Model*. Working Paper, Alfred P. Sloan School of Management, MIT, Cambridge, Massachusetts.
Shermer M. (2008). *Why Our Brains do not Intuitively Grasp Probabilities*. Scientific American 1 September 2008.
Schröder-Hinrichs J-U., Hollnagel E. and Baldauf M. (2012). *From Titanic to Costa Concordia—a Century of Lessons not Learned*. Journal of Maritime Affairs 11 pp. 151-167.
Schrödl H. and Turowski K. (2014). *Risk Management in Hybrid Value Creation*. Decision Support Systems 58 pp. 21-30.
Schroedel J. (2019*). Radical vs Incremental Change: What is the Difference?* Citizenlab, 10 December 2019.
Schultz M.T., Mitchell K.N., Harper B.K., and Bridges T.S. (2010). *Decision Making Under Uncertainty*. ERDC TR-1012 Engineer Research and Development Center, US Army Corps of Engineers. Vicksberg MS.
Schweizer P-J. (2018). *Systemic Risks – Concepts and Challenges for Risk Governance*. Journal of Risk Research, 24:1, 78-93, DOI: 10.1080/13669877.2019.168757
SCV (2022). *Guide for Inclusive Community Consultations*. Safer Care Victoria, June 2022. Government of Victoria, Melbourne, Australia.
Sebas S. (2023). *Beyond Continuous Improvement: Embracing Change for a Brighter Future*. LinkedIn, 18 May 2023. Accessed at: https://www.linkedin.com/pulse/beyond-continuous-improvement-embracing-change-brighter-sergio-sedas/.
Seddon J. (1997a). *Ten Arguments Against ISO 9000.* Managing Service Quality 7(4) pp. 162–168.
Seddon J. (1997b). *In Pursuit of Quality: The Case against ISO 9000*. Oak Tree Press, Twickenham, UK.
Seet C. (2020). *Capability-Based Planning vs. Traditional Project Planning Approaches*. Jibility, Accessed at: https://www.jibility.com/capability-based-project-planning-approach/.

Seymour B., Daw N., Dayan P., Singer T., and Dolan R. (2007). *Differential Encoding of Losses and Gains in the Human Striatum*. Journal of Neuroscience 27 pp. 4862-4831.
Shang K. **(2014).** *Inconsistent Inference in Qualitative Risk Assessment*. 2014 CAS in Focus.
Singh M., Fosselie T., and Wiggen F. (2010). *Data Information, Knowledge and Decision-Making in Condition Monitoring*. Proceeding of the 23rd COMADEN Conference, Nara, Japan.
Standards Australia (2023).
Sillmann J., Christensen, I., Hochrainer-Stigler, S., Huang-Lachmann, J., Juhola, S., Kornhuber, K., Mahecha, M., Mechler, R., Reichstein, M., Ruane, A.C., Schweizer, P.- J. and Williams, S. 2022. *ISC-UNDRR-RISK KAN Briefing Note on Systemic Ris*k, Paris, France, International Science Council, DOI: 10.24948/2022.01.
Sivitskil A. and Põodra P. (2021). *Risk Assessment and Calibration of Risk Matrices Aspects*. IOP Conf. Ser.: Mater. Sci. Eng. 1140 012040.
Slabaugh R.M (2000). *Enterprise Risk Management: Realizing Profit from Risk*. 46th Annual Tax Conference. Accessed at: https://heinonline.org/HOL/LandingPage?handle=hein.journals/antcwilm40&div=15&id=&page=.
Smithson C.W. (1998). *Managing Financial Risk: A Guide to Derivative Products, Financial Engineering, and Value Maximisation*. McGraw Hill, Boston MA.
Snow D. (2018). *Siege: The Powerful and Uncompromising Story of What Happened Inside the Lindt Cafe and Why the Police Response Went So Tragically Wrong*. Allen and Unwin, Crow's Nest. NSW Australia.
Snow D., Ralston N., and Benny-Morrison A. (2016). *Lindt Café Siege Inquest Exposes Crisis of Leadership in NSW Police.* The Sydney Morning Herald 20 August 2016. Accessed on 24 April, at:
http://www.smh.com.au/nsw/there-is-a-crisis-of-leadership-in-the-nsw-police-20160818-gqw8f5.html.
Sotani A. and Izquierdo A. (2019). *Adaptive Learning Under Expected and Unexpected Uncertainty*. Nature Reviews Neuroscience 20 pp. 635-644.
Special Commission (2020). *Special Commission of Inquiry into the Ruby Princess* Report, August 2020. Government of NSW, Sydney, Australia.
Sperling H.D. (2000). *Expert Evidence: The Problem of Bias and Other Things*. Judicial Review 4(4) p. 429-462.
SRA (2018). *Society for Risk Analysis Glossary*. Updated August 2018.
Starcke K. and Brand M. (2012). *Decision Making Under Stress: A Selective Review*. Neuroscience & Behavioural Reviews 36(4) pp. 1228-1248.
Standards Australia (1995). *Australian New Zealand Standard. Risk Management. AS/NZS 4360: 1995*. Standards Australia, Sydney.
Standards Australia (2020a). *SA HB 436.1: 2020 Risk management guidelines – Companion to AS ISO 31000:2018. Part: Boards and Executives*. Standards Australia, Sydney.
Standards Australia (2023b). *AS HB 167: 2023 Managing disruption-related risk*. Standards Australia, Sydney.
Stanton N.A., Salmon P.M., Rafferty L.A., Walker G.H., Baber C., and Henkins D.P. (2013). *Human Factors Methods: A Practical Guide for Engineering and Design*. Second edition, Ashgate Publishing, Farnham, UK.
Stergiopoulos G., Kotzanikolaou P., Theocharidou M., and Gritzalis D. (2015). *Risk Mitigation Strategies for Critical Infrastructures Based on Graph Centrality Analysis*. International Journal of Critical Infrastructure Protection 10 pp. 34-35.
Stevens J., Moultrie J. and Crilly N. (2008) *Designing and Design Thinking in Strategy Concepts: Frameworks Towards an Intervention Tool*. In: Design Thinking: New Challenges for Designers, Managers and Organizations, 14-15 April 2008, Cergy-Pointoise, France.
Stulz R.M. (2009a). *Six Ways Companies Mismanage Risk*. Harvard Business Review, March 2009 pp. 1-7.
Stulz R.M. (2009b). *Risk Management Failures: What Are They and When do They Happen?* Cornerstone Research, Boston, MA.
Taylor M.J., McNicholas C., Nicolay C. Darzi A., Bell D., and Reed J. (2014). *Systematic Review of the Application of the Plan-Do-Study-Act Method to Improve Quality in Healthcare*. BMJ Quality and Safety 23 pp. 290-298.
Tebehaevu O.J. (2015). *Modeling Decision Making Determinants.* Thesis, East Carolina University.
Tepetepe G., Simenti-Phiri E., and Morton D. (2022). *A Survey Comparative Analysis of Cartesian and Complexity Science Frameworks Adoption in Financial Risk Management of Zimbabwean Banks*. Quantitative Finance and Economics 6(2) pp. 359-384.
Terziovski M., Power D., and Sohal A. (2003). *The Longitudinal Effects of the ISO 9000 Certification Process on Business Performance*. European Journal of Operational Research 146(3) pp. 580– 595.
Thomas P., Bratvold R.B., and Bickel J.E. (2014). *The Risk of Using Risk Matrices*. SPE Economics and Management, April 2014 pp. 56-66.
Toma S.-G., Marinescu P. and Grāinaru C. (2016). *Strategic Planning and Strategic Thinking*. Revista Economicā 68(5) pp. 168-175.

Toor S. and Ofori G. (2008). *Leadership versus Management: How They Are Different, and Why*. Leadership in Management and Engineering 8(2) pp. 61-71.
Tophoff V. (2014). *A Ball of Confusion: What is Your Appetite for Risk Appetite*? International Federation of Accountants, 18 June 2018. Accessed at: https://www.ifac.org/knowledge-gateway/contributing-global-economy/discussion/ball-confusion-what-your-appetite-risk-appetite.
Tosey P.C., Visser M., and Saunders M.N.K. (2012). *The Origins and Conceptualisations of `Triple-loop' Learning: A Critical Review*. Management Learning 43(3) pp. 289-305.
Trimmer P.C., Houston A.I., Marshall J.A.R., Mendl M.T., Paul E.S., and McNamara J.M. (2011). *Decision-making Under Uncertainty: Biases and Bayesians*. Animal Cognition 14 pp. 465-476.
Tukel O.I. and Rom W.O. (2001). *An Empirical Investigation of Project Evaluation Criteria*. International Journal of Operations & Production Management. 21(3) pp. 400-426.
Turner J.R., and Baker R.M. (2019). *Complexity Theory: An Overview with Potential Applications for the Social Sciences.* Systems 7(1) https://doi.org/10.3390/systems7010004.
Tversky A. and Kahnemann D. (1974). *Judgement Under Uncertainty: Heuristics and Biases*. Science 185(4157) pp. 1124-1131.
UFMCS (2016). *The Applied Critical Thinking Handbook, 8.1 September 2016*. TRADOC G2 Operational Environment Enterprise, Center for Applied Critical Thinking, University of Foreign Military and Cultural Studies. Ft Leavenworth, KS.
Ülkümen G., Fox C. R., and Malle B. F. (2016). *Two Dimensions of Subjective Uncertainty: Clues from Natural Language*.
UNEP (2020). *Handbook for Stakeholder Engagement at the United Nations Environment Program (UNEP).* United Nations Non-Governmental Liaison Service and UNEP Civil Society Unit.
US EPA (2023). *Risk Management*. United States Environmental Protection Authority. Accessed at: https://www.epa.gov/risk/risk-management#tab-2.
van der Heijden K., Bradfield R., Burt G., Cairns G., and Wright G. (2002). *The Sixth Sense: Accelerating Organisational Learning with Scenarios.* John Wiley & Sons, Chichester, UK.
Van der Veght G.S., Essens P., Wahlstrom M., and George G. (2015). *Managing Risk and Resilience*. Academy of Management Journal 58(4) pp. 971-980.
Van Hoorde K., Van Huffel S., Timmerman D., Bourne T., and Van Calster B. (2014). *A Spline-based Tool to Assess and Visualize the Calibration of Multiclass Risk Predictions*. Journal of Biomedical Informatics
Van Kemenade E. (2014). *The Myth of the PDCA-Cycle in Time of Emergent Change*. Proceedings of the Conference: European Organisation for Quality Congress, June 2014, Goteborg, Sweden.
Vaughn D. (2016). *The Challenger Launch Decision: Risk Technology, Culture and Deviance at NASA*. The University of Chicago Press, Chicago, IL.
Veazie S., Peterson K., and Bourne D. (2019). *Evidence Brief: Implementation of High Reliability Organization Principles*. VA Evidence Synthesis Program. Veterans Affairs, Washington DC.
VicGov (2022a). Human-centred Design Playbook. Government of Victoria, Melbourne, Australia. Accessed at: https://www.vic.gov.au/download-human-centred-design-playbook
VicGov (2022b). *Set up a Public Consultation Project on Engage Victoria – Digital Guide*. Victorian Government. Accessed at: https://www.vic.gov.au/Set-up-a-public-consultation-project-on-Engage-Victoria-digital-guide
Villa V., Paltrinieri N., Khan F., and Cozzani V. (2016). *Towards Dynamic Risk Analysis: A Review of the Risk Assessment Approach and its Limitations in the Chemical Process Industry*. Safety Science 89 pp. 77-93.
Viscelli T.R., Hermanson D.R., and Beasley M.S. (2017). *The Integration of ERM and Strategy: Implications for Corporate Governance*. Accounting Horizons 31(2) pp. 69-82.
Voicu I., Panaitescu F.V., Panaitescu M., and Turof M. (2018). *Risk Management with Bowtie Diagrams*. ModTech 2018, IOP Conf. Series: Materials Science and Engineering 400 Article 082021.
Vuillermin F. and Huck-Sandhu S. (2021). *Strategic Planning in Dynamic Environments: How Design Thinking Can Complement Corporate Communication*. Journal of Design Thinking 2(2) pp. 85-96.
Vuorinen S. (2022). *Monitoring of the Operating Environment and Foresight Activities to Support Strategic Decision-making*. National Audit Office of Finland, 8.11.2022.
Wardman J.K. (2020). *Recalibrating Pandemic Risk Leadership: Thirteen Crisis Ready Strategies for COVID-19*. Journal of Risk Research 23(7-8) pp. 1092-1120.
Walker W.E., Haasnoot M., and Kwakkel J.H. (2013). *Adapt or Perish: A Review of Planning Approaches for Adaptation Under Deep Uncertainty*. *Sustainability* 5(3) pp. 955- 979.
Walker W.E., Lempert R.J., and Kwakkel J.H. (2016). *Deep Uncertainty. In:* Encyclopedia of Operations Research and Management Science 3rd Edition (Editors: S.I. Gass and Fu M.C.), Springer, New York.

Weick K.E. and Sutcliffe K.M. (2015). *Principle 5: Deference to Expertise*. In: Managing the Unexpected, Wiley New York, NY.
Weick K.E. and Sutcliffe K.M. (2007). *Managing the Unexpected: Resilient Performance in an Age of Uncertainty*. Jossey Bass, Wiley.
WHO (2022). *WHO Foresight: Monitoring Emerging Technologies and Building Futures-thinking*. World Health Organisation, Geneva, Switzerland.
Willumsen P. Oehmen J., Stingl V., Geraldi J. (2019) *Value Creation Through Project Risk Management*. International Journal of Project Management 37(5) pp. 731-749.
Wolfe J. (2014). *The Speed of Risk. COSO 2013 & How to Protect Your Enterprise Against Today's Biggest and Fastest Threats*. Resolver June 11-13th.
Wolters and Kluwer (2015). *What is Risk Velocity and Should You Track It?* Expert Insights, Legal, Compliance, ESG, 7 October, 2015.
Wolters and Kluwer (2022). *Why are Human Factors so Important in Risk Assessment?* Wolters and Kluwer, 16 May 2022. Accessed at: https://www.wolterskluwer.com/en/expert-insights/why-are-human-factors-so-important-in-risk-management.
Woodell G., Gramling R., and Forsyth C.J. (2002). *A Method for Modelling Low Probability-High Consequence Risk Events: Vessel Traffic on the Lower Mississippi River*. Pierce Law Review 1(1/2), pp. 85-101.
Woods M., Dowd K., and Humphrey C. (2008). *The Value of Risk Reporting: A Critical Analysis of Value-at-risk Disclosures in the Banking Sector.* International Journal of Financial Services Management 3(1) pp. 45-64.
Wright A. (2010). *Public Service Quality: Lessons Not Learned*. Total Quality Management 8(5) pp. 313-320.
Wu Y.A. and Saunders (2011). *Governing Information Security: Governance Domains and Decision Rights Allocation Patterns*. Information Resources Management Journal 24(1) pp. 28-24.
Xi Y., Xiong Z., Dong X., and Lu H. (2017). *Risk Assessment and Decision-Making under Uncertainty in Tunnel and Underground Engineering.* Entropy 19 Article 549.
Xiaolei Z. and Paraskevas A. (2011). *Risk Appetite: How Much do We Know About it*. In: Proceedings of the 1st International Conference in Safety and Crisis Management in the Construction, Tourism and SME Sectors (1st CoSaCM) (Editor: G. Boustras and N. Boukas). European University Cyprus Cultural Center, Nicosia, Cyprus, 24-28 June 2011.
Xueca*i* X. and Deyon G. (2018). *Human Factors Risk Assessment and Management: Process Safety in Engineering*. Process Safety and Environmental Protection 113 Pages 467-482.
Yilmaz A.K. (2019). *Strategic Approach to Managing Human Factors in Aircraft Maintenance Organization: Risk Mapping*. Aircraft Engineering and Aerospace Technology 91(4) pp. 654-668.
Yu A.J. and Dayan P. (2003). *Expected and Unexpected Uncertainty. ACh and NE in the Neocortex*. Advances in Neural Information Processing Systems 15 pp. 157-164.
Yuthas K., Dillard J.F., and Rogers R.K. (2004). *Beyond Agency and Structure*. Journal of Business Ethics 52 pp. 229-243.
Zhou P. and Leung H. K. N. (2012*). An Integrated Risk Analysis Method Using Spatial Interpolation*. 19th Asia-Pacific Software Engineering Conference, Hong Kong, China, 2012, pp. 452-461
Zhou W.C. and Sun S.L. (2020). *Red Teaming Strategy: Huawei's Organizational Learning and Resilience*. In: Huawei Goes Global Vol. 2: The Regional, Geopolitical Perspectives and Crisis Management. Palgrave Macmillan.
Zobel T. (2015). *ISO 14001 Adoption and Industrial Waste Generation: The Case of Swedish Manufacturing Firms*. Waste Management and Research: The Journal for a Sustainable Economy 33(2) pp. 107-113.
Zobel T. (2018). *ISO14001 Adoption and Environmental Performance: The Case of Manufacturing in Sweden.* In: ISO9001, ISO14001, and New Management System Standards pp. 39-58, (Editor: I. Heras-Saizatbitoria), Springer, Cham, Switzerland.
Zohar A., Jackson C., and Partridge K. (2005). *From Words to Action, vol. 1: Practitioners' Perspectives on Stakeholder Engagement.* United Nations Environment Programme.