UNIVERSITY OF Southampton

Risk Intelligence Production on Complex Projects:

practical discussion points

FOREWORD

One of the Centre for Risk Research's (CRR) key aims is to provide thought leadership in the field of risk management, and an important mechanism for achieving this aim has been through the production of several discussion and guidance documents. This latest edition to this series of CRR discussion documents examines the production of risk intelligence in the context of complex projects and is the first of our discussion documents to have been developed in collaboration with colleagues in Southampton Business School's Centre for Applied Science in Project Management (CentasPM). This collaboration has enabled the document's authors to draw upon their multidisciplinary expertise to incisively evaluate and highlight how risk intelligence can be generated and utilised to enhance the management of risk in complex and fluid multi-stakeholder projects. This discussion topic is particularly pertinent in an age in which there is an ever growing volume of accessible intelligence information and a diverse range of information sources, and in which complex projects are often characterised by fluid budgets, increasing time pressures, changing objectives, greater scrutiny and accountability, and socio-economic uncertainties. This CRR discussion document explains how this array of challenges to a project's success can be more effectively navigated using formalized and professional risk intelligence production and management approaches. More generally, we hope that the document will be of interest to all managers who deal with information and that it will convince anyone involved in managing projects that the production and utilisation of intelligence information should be a central part of their risk management activities. We are confident that you will find the ideas and guidance in this document stimulating and informative, and we welcome your feedback.

Dr Ian Dawson
Director of the Centre for Risk Research

In order to advance the risk profession we must bring together rigorous academic enquiry with practical real world experience. This work from the team at Southampton University gives us some new language and thinking to address issues of risk, complexity and decision-making that are very much required in a world where we need complex projects and extended enterprises to succeed in delivering sustainable growth. We commend this new thinking and look forward to hearing how it progresses.

Carolyn Williams CMIRM, ACII
Director of Corporate Relations, Institute of Risk Management

AUTHORS

Dr Alasdair Marshall (Centre for Risk Research)
Dr Serkan Ceylan (Centre for Applied Science in Project Management)

CONTRIBUTING EDITOR

Dr Ian Dawson (Centre for Risk Research)
Dr Mario Brito (Centre for Risk Research)

Co-published in 2020 by the Centre for Risk Research and the Centre for Applied Science in Project Management, University of Southampton.

INTRODUCTION

This discussion document is a joint effort from the Centre for Risk Research (CRR) and the Centre for Applied Science in Project Management (CentasPM), both situated at Southampton Business School. Its purpose is to generate – and to some limited extent within the pages available, speak to - a list of challenging discussion points on *risk intelligence production*. Recognising the need for some flexibility in allowing readers themselves to form a view of exactly what should differentiate risk intelligence production from other similar and overlapping practices, we concentrate on drawing attention to a range of matters which we think managers need to consider to achieve proficiency. Professionalism in risk intelligence production, as we perceive it in very broad outline, comprises professionalism in handling information in general and risk information especially. It also extends to encompass what we will call *risk knowledge* development. We explain how this professionalism may be achieved through the application of some very relevant ideas and practices from the intelligence management and knowledge management disciplines.

We take as our application context organisations generally but projects predominantly. Throughout the document we represent risk intelligence effort as likely to deliver its strongest and starkest benefits when used to enhance the management of complex and fluid multi-stakeholder projects where chaos and unpredictability are particularly rife, entailing that time/information poverty and surprise all matter frequently as disturbances and challenges to managers.

In advocating for a distinctive professional approach to risk intelligence production, we also have in mind leadership and management coordination challenges for larger projects in particular. Arguably, the larger the project, and hence the more globally scaled the stakeholder management issues, the more challenging it becomes to manage intelligence information effectively across what we might summarily call (inter)organisational, geographical, social, cultural and even geopolitical distance. The *confidentiality, credibility, source reliability* and even the *meaning/significance* of pertinent risk information, may all demand more careful attention as these distances co-increase. Yet how often are these interrelated practical issues discussed as mattering for effective risk management? Almost never, we would suggest. We plug this professional knowledge gap by advocating for explicit consideration of these basic information management issues within professionalised risk intelligence production.

It makes good sense, we believe, to focus discussion of innovative management practice towards where it can provide the quickest, easiest and greatest wins. We regard risk intelligence as having most to offer within the challenging circumstances outlined above. Correspondingly we envision a readership primarily comprising Project Managers who must deal with risk, and with what for now we loosely term the *intelligence information* upon which risk management is based, under these circumstances.

And yet our document also sits within the literature tradition, well established at Southampton Business School, recognising project risk management as a crucible for ideas and practices that can benefit organisational risk management more generally. Rationales for this project crucible approach are fascinating in their own right. Very generally speaking, our thinking here is that the best organisational risk management solutions are likely to be those that deal effectively with the more intensive irregularity and unpredictability that are encountered within day-to-day project risk management. This entails we also regard organisational risk management professionals and students as making up an important part of our intended readership. Furthermore, as we will soon explain, this discussion document should be of interest to all managers who must deal with information, especially under the challenging circumstances we have sketched out above. The hiatus between managing different forms of information and managing risk, we will argue, has persisted for far too long.

"The University of Southampton's Risk Intelligence Production on Complex Projects briefing draws on the 10 pertinent discussion points for private and public businesses to survive in a VUCA world, namely volatile, uncertain, complex and ambiguous environments. An important perspective not given sufficient weighting is the notion that someone's risk is another's opportunity. Different market actors will have different perspectives on the same available data and information in the public domain. It is that business' or public organisation's ability to process that into an insight relative to that business' context, strategy and capabilities and limitations that will define it as a risk or an opportunity. One point not highlighted enough is that of business culture and the notion of blind spots. The risk intelligence programme and process needs to have stakeholder support from that part of the business which has the mandate to act on the Insight. The risk intelligence process should also look to provide a set of recommendations with respect to how to mitigate the risk or accelerate the opportunity. Otherwise risk intelligence becomes a passive activity as the business goes from one set of rocks to another in pursuit of its goals for customers, shareholders and employees."

Andrew Beurschgens
Volunteer UK Chapter Chair
Strategic and Competitive Intelligence Professionals (SCIP)

WHAT IS RISK INTELLIGENCE PRODUCTION?

Here we return immediately to the nature of our basic subject matter, and indeed to the problems that arise as soon as we consider prospects for simple definitions and clarifications of precisely what is at issue. Risk intelligence is an expression which most readers will doubtless be unfamiliar with. It brings together two terms, *risk* and *intelligence*, both of whose meanings are widely and strongly contested. A (2017) CRR discussion document entitled '*Risk Intelligence'* has already laid our groundwork by exploring what this expression means in some scattered literatures that use it. To summarise briefly, that preliminary discussion document focussed on the idea that risk management needs to get smarter and more proactive in dealing with competitive and adversarial social threat, for example by drawing on the services, skills and techniques of competitive intelligence professionals. On that view, organisations become *risk intelligent* by seeking, collecting, analysing and applying *risk intelligence information* within *risk intelligence processes*. The (2017) CRR document also pointed out that this organisational concept of *risk intelligence* should not be confused with the individual psychology concept of measurable *risk intelligence* - or RQ, analogous to IQ – which regards high RQ individuals as avoiding false certainty for erroneous probability estimates. Nonetheless it was suggested that there are very worthwhile debates to be had, regarding why effective risk intelligence production hinges on a professional management attitude manifesting high RQ. The idea that high RQ favours an open minded and inquisitive risk imagination, which can be considered a psychological cornerstone for professionalised intelligence work across all military and business domains, comes strongly to mind here.

The above view of risk intelligence suggests risk management practice enhanced through intelligence management professionalism, where risk intelligence information may differ from risk information *per se,* very straightforwardly because it is sourced through professionalised intelligence work. This simple view of risk intelligence may provide a good initial understanding, and it may prove practically useful for managers in many different situations. However, confusion may quickly arise when we contemplate the varying meanings of *risk*, *intelligence* and *information*, and ask how (*risk*) *intelligence* might be regarded as differing from (*risk*) *information*. There are potentially many different permutations of meaning to explore here. The development of a theory of risk intelligence by reviewing and choosing from all the permutations that arise by varying the meanings of these three terms would be well beyond the scope of this document. One obviously relevant complication we cannot ignore, however, is that risk is nowadays typically viewed as encompassing both threat and opportunity. We heed this common language usage issue by incorporating within our conceptualisation of *risk intelligence production* a fourth information management concept, *insight*. Recognising that information management undertaken by marketing (or *marketing intelligence*) professionals in particular, has rendered *insight* a prominent management concept treating knowledge as a source of competitive advantage, we will explicitly consider insight processes as helpful for managing risk intelligence in its positive *opportunity* aspect.

We also recognise a need to offer some practical working clarity on what makes producing *risk intelligence* different from routinely pushing risk information through generic risk management processes. We certainly cannot bring closure to the longstanding *intelligence* vs *information* debate here. Furthermore we should emphasise that even the most basic definitions and boundaries at issue remain contested and vexing for intelligence professionals. Of course, however, it is important to heed the connotations whereby intelligence is often considered as something that is gathered through the application of some combination of stealth and audacity, and whose use may then require secrecy and security.

Risk intelligence work might therefore usefully be viewed as requiring exemption from the principle of *transparency* that characterises much risk management guidance. This principle clearly has much to offer in organisational circumstances that permit it to exist. Indeed its importance is widely recognised in risk management guidance (e.g. as a clause 3 guiding principle in ISO 31000). Nonetheless there remains the counter-argument that transparency does need to be reined in on occasion to reflect the everyday risk management reality whereby risk managers must sometimes gather and communicate risk intelligence whose divulgence either generally or to the wrong parties might be unwise, or indeed unethical in cases where it is important to protect sources.

Our earlier (2017) CRR discussion document laid these same emphases on stealth, audacity, secrecy and security by focussing on risk intelligence practice as involving the direction-collection, analysis and use of sensitive and confidential information pertaining to *social threat* as opposed to threat in general. Working from that perspective, risk imagination becomes central to risk intelligence work, simply because anticipating the (often deliberately concealed) motives, strategies and resources of adversaries might all too easily stretch the risk imagination beyond its limit. Notably, this view of *risk intelligence production* emphasising the importance of *risk imagination,* chimes with the popular view which regards *failure of imagination* as frequently the most fundamental cause of intelligence failure. This idea is popularly associated with its military intelligence use to explain such events as the Pearl Harbour and September 11 attacks on the US, yet its relevance for managing novel and non-routine risk on projects and in organisations is obvious.

We carry forward that view of *risk intelligence* – while further drawing on the also commonplace view of intelligence work as making provision for routine scanning of public domain information sources such as newspapers and magazines. What this view brings to the table is its recognition that valuable intelligence information may often hide in plain sight, or at least be accessible if the will and resources are there to proactively scour the information environment for it. On this view, intelligence work is to a considerable extent concerned with applications of creative imagination to tasks of *pattern recognition* or *joining the dots* for information that is either presently available or accessible. We can certainly count such aptitude as an important component of the risk imagination necessary for risk intelligence work.

Summing up, then, and not wishing to impose any unnecessary restriction on what the expressions *intelligence* and *risk intelligence* can usefully be understood to mean, we suggest that it might often prove healthy to merge the meanings of (risk) intelligence and (risk) information for many practical purposes. An important consideration within our thinking here is that *both* can be viewed as requiring conveyance through formal processes where meaning/significance and use value, although not clear from the outset, are progressively and systematically resolved. Nonetheless, we recognise that the following very challenging question inevitably arises with all risk intelligence practice in organisations and on projects:

Discussion Point 1: Risk intelligence work is likely to benefit greatly from organisational/project definitions of risk intelligence which clarify its unique nature and contribution within the context of broader management practice.

We hope that managers will be in a stronger position to suggest effective working definitions after reading the remainder of our document. The greater challenge within the above question is, of course, that of what risk intelligence production is best understood as referring to in organisational process and infrastructure terms. The (2017) CRR document resolved this issue by advocating use of a *boosted risk radar*. This expression was used to refer to greater use of proactive intelligence gathering and simulation techniques as plug-ins to enhance existing resilience and risk identification practices in organisations. This amounted to a very simple solution – helpful to a considerable extent and yet arguably insufficient for a professional understanding of risk intelligence which seeks to optimise its contribution.

In the present document, therefore, we attempt to dig deeper by discussing risk intelligence practice as occurring not just at the interface of risk management and competitive intelligence, but rather at multiple interfaces where managing risk, and managing across the whole gamut of *information*, *intelligence*, *knowledge*, and even *insight*, all intersect. We have no desire to propose a consolidated process solution covering the management of all these areas. However, we will discuss risk intelligence production and use in terms of the managerial dexterity required to traverse this broad territory comprising diverse epistemic challenges which demand professionalised management attention for a whole variety of reasons that are likely to overlap considerably with those of risk management. Our key point here, and indeed our second discussion point, can be summarised as follows:

Discussion Point 2: Risk intelligence information is best managed through smart and targeted engagement with diverse information management activities.

Looking from this perspective, risk intelligence information can be sourced from absolutely anywhere, which is to say, from right across the internal and external informational contexts of the managed entity. Some obvious sources include financial/loss/performance/audit data. Then of course there is the informational yield from competitive/business/marketing intelligence work. By already bearing the *intelligence* stamp, this may provide managers with their primary basis for reflection on what makes intelligence information different from other kinds of information. Yet everyday hearsay about what is happening in the complex social world may also prove an important source; indeed, so might information about all sorts of novel/unexpected occurrence. Even very *weak signals* hinting at conceivably any kind of possibly impending threat, may also be counted as actionable risk intelligence information by managers, especially by those managers who aspire towards providing the enhanced resilience associated with high reliability organisations. Hence our general conclusion to round off this section is, as per the above discussion point, that risk intelligence production must be concerned with the smart and targeted sourcing of risk intelligence from many sources. However, this begs the question of how to recognise it in the first instance. We focus on this question next.

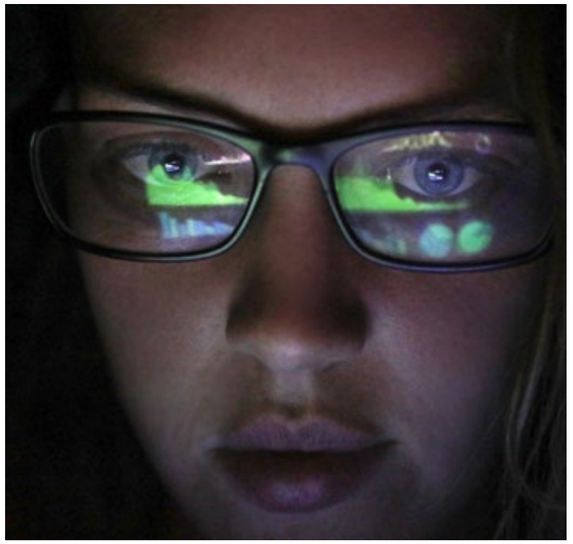
WHEN MANAGING INFORMATION BECOMES MANAGING RISK INTELLIGENCE

Arguably what matters *in the first instance* to trigger risk intelligence management is as follows: when first encountering all sorts of information and scrutinising it for its possible value, it should be second nature for managers to engage their risk imagination to explore whether that information either serves to establish, or helps to build a more detailed understanding of, some causal risk story logically conjoining root causes to effects that matter. Ideally some clear understandings of who or what is *exposed* to the risk, and indeed what makes them or it *vulnerable* to the risk, may usefully be incorporated within these risk stories. Some recognition of existing risk controls, if there are any, might also be recognised. Risk matrices, comprising risk categories used on a project or within an organisation, may sometimes provide very helpful context within which to develop these stories, for example by aligning them to managerial accountabilities expressed as risk ownerships. We would suggest that as soon as the seed of some distinctive risk story begins to grow, no matter whether this takes the form of an *abstract-theoretical* story of a risk that might happen, or of a more *concrete-experiential* story for a risk that seems to be in the making, then at this point we would say that *risk information*, over and above simply *information*, is at issue.

Next, we need to explain our view that at such junctures it is best to conceive of the management challenge as being to manage *risk intelligence information* and not just *risk information*. Our basic point here is that this additional reference to *intelligence* can provide a trigger for applying an enhanced professionalism in the day-to-date handling of risk information. The structure we follow in the remainder of our document is one which explores this enhancement as a co-injection of *intelligence management professionalism* and *knowledge management professionalism*. To prepare the reader we can very briefly summarise these management enhancement issues as follows:

- Consider the *intelligence cycle* and similar information management processes for what they can contribute to the ongoing development and use of risk knowledge;
- Consider *credibility* and *source reliability* when evaluating the risk intelligence information upon which risk knowledge is based;
- Consider the development and use of both *explicit* and *tacit* risk knowledge;
- Consider the development and use of both *abstract* and *concrete* risk knowledge.

We explore these matters sequentially while also drawing attention to some of their more interesting interrelationships. In this way we aspire towards a holistic appreciation of how best to manage risk intelligence whenever and wherever it is encountered within the broader informational milieu. What results, essentially, is a view of risk intelligence production centred on a managerial dexterity for more enlightened handling of risk information and knowledge across many different project and organisational contexts.



MANAGERIAL DEXTERITY FOR RISK INTELLIGENCE PRODUCTION

Risk intelligence production, to recapitulate, can be viewed as hinging upon a managerial dexterity for navigating complexities of existing process and infrastructure in order to create organisational value from what we very loosely term *risk intelligence information*. Drawing on knowledge management theory, we will soon explore how information can be converted into *knowledge*. This concern will lead us, in turn, to look in some detail at what it can mean to develop *risk knowledge* at higher levels of knowledge complexity. Accordingly, our vision of professionalism in risk intelligence production is very fundamentally based on conceptual wherewithal for scrutinising and developing risk knowledge at higher levels of complexity.

Another important consideration when exercising managerial dexterity for risk intelligence production is, we suggest, an appreciation that it may often be unhelpful to fully split-off risk intelligence information from business intelligence information, competitive intelligence information, marketing intelligence information, and indeed all those information flows that do not go under the intelligence heading. Rather, what matters is an appreciation that there is always just *information* leading to *knowledge*, must be conveyed through appropriate organisational pathways to where its value can be fully realised. It is likely that information will often lend itself to expression in risk terms – especially when risk stories begin to take shape and where prudence discerns that existing management controls for the perceived risks are absent or insufficient. However, this may not always be the best way forward for developing and applying knowledge.

We propose that when to use the language of *risk*, and when to use some other language, such as that of *marketing*, *strategy*, *finance or performance*, and indeed how best to mix these languages together to produce hybridised discourses which best address the issues at hand, can be regarded as matters of professional judgment. Favoured solutions will vary enormously. Nonetheless we suggest that managerial dexterity for risk intelligence, by entailing a familiarity with *risk knowledge* in particular, can only enhance professional judgments about how best to capture the meaning and use value of information.

Simplifying down, and at the risk of establishing a false binary, we might also say that the production of risk intelligence is *always* about managing risk, *at one end*, and managing information/intelligence/knowledge/insight *at the other end*. This rhetorical contrivance, which presents risk intelligence production effort as always being firmly rooted *at both ends*, is one that we tentatively regard as offering some practical guidance value. Risk intelligence production, theorised as selective and efficient use of process/infrastructure, non-routine communication between multiple process owners, and process/infrastructure hybridisation, must surely benefit from a managerial dexterity which explores the practical issues arising *from both of these ends*. Surely there is no such thing as risk information *per se,* whose value can only be realised by channelling it through risk management processes. To suggest that in reality there is only ever just *information* and *knowledge*, which always deserves consideration at its risk *end*, is in effect to become critically awakened to an important academic and professional hiatus between managing risk and managing the conversion of all sorts of information into useful knowledge and insight. In this discussion document we will try to bridge these academic and professional domains, thus addressing the following question:

Discussion Point 3: Knowledge management has fundamental concerns with sourcing, developing, communicating, applying and retaining knowledge in many forms. Its implications for developing risk intelligence production as a professionalised management activity are enormous.

Our discussion will seek to show the way forward on bridging risk management and knowledge management practice within organisations, at least within the domain of risk intelligence production which is our central concern, and in particular by drawing attention to helpful distinctions between *tacit* vs *explicit* and *abstract* vs *concrete* risk knowledge. We hope that, upon reading to the end of our document, some readers may even feel that their basic thought process for thinking about risk within organisations and on projects has been transformed through an infusion of useful ideas from the knowledge management discipline.

RISK INTELLIGENCE PRODUCTION AT CLOCK SPEED

Our focus is on how to produce risk intelligence to increase overall project success – with an emphasis on managing at clock speed (i.e. in real time and often with urgency). In this section we develop our rationale for selecting this clock speed emphasis. Here it becomes important to recapitulate that our formulation of professionalism in risk intelligence production takes the form of a simplifying *managerial dexterity.* We envision this dexterity as arising with an appreciation that it is important to consider a particular range of matters *at clock speed* whenever information becomes available for consideration in its risk aspect. And we further view this concern as a foundation for the ongoing developing of a skilled professional habit characterised by rigour in information handling, applied to risk information and risk knowledge development in particular. We explore the range of pertinent matters which we have in mind from the next section onwards. However, as a final preliminary we use the present section to reflect some more on why this approach may offer real benefit to managers in their daily working lives.

In our introduction we made the point that project managers especially, and to a lesser extent managers across organisations generally, will frequently encounter real-time management challenges characterised by novelty, complexity, fluidity and urgency. This entails that the often meagre and perhaps sometimes misleading risk information that becomes available, needs to be handled very carefully. Risks don't wait politely in queues to be attended to. Professionalism for handling risk urgently, at clock speed, clearly matters – and surely that professionalism needs to encompass the effective handling of information and knowledge. And yet at this juncture it becomes interesting to reflect that best practice and compliance related guidance for organisational risk management remains pitched far more at committee pace than at clock speed. Furthermore it has very little to say about information and knowledge *per se*. This begs the following question:

Discussion Point 4: Guidance on risk management needs to move away from formal process and focus more on shaping the managerial dexterity necessary for the lean and effective handling of risk intelligence, in real time, within complex project environments.

Some more detailed grounds for thinking along these lines are as follows. Managers working on complex projects are likely to learn, sooner or later, that they are going to be surprised by the flow of events, and, as a necessary corollary to that, by the actionable intelligence information that becomes available before, during and after surprising events. Such managers will often have cause to reflect, with powers of retrospect, that it may have advantaged them to have been more proactive in gathering any intelligence information that has eventually proven to matter. Similarly, they might well wish that they were more knowledgeable about the range of information analysis and management options available, or indeed which it would make sense to establish or hybridise. In other words, they should have cause to greatly value managerial dexterity in risk intelligence production.

Notably, a range of psychological issues become important at this juncture under the broad heading of what Alvin Toffler (1970) famously called *information overload*. Much project management literature discusses failure to filter and retain high value information as both *emerging from* and *as producing* patterns of stress, low productivity, and what is sometimes termed *information fatigue syndrome*. This places a premium on the creation of good guidance aimed at building professional confidence, partly in its psychological wellbeing aspect, in order to stave off this syndrome and all the damage it may cause. An interesting question arising at this juncture is just how many practicing project managers would express the following view:

Discussion Point 5: Information fatigue is a common cause of failure in project risk management. A lean and effective approach to risk intelligence production may well be the solution.

In pursuing this solution, we postulate that any practical guidance we can offer, to help project managers become more effective in dealing with risk intelligence information under difficult project circumstances, may well offer interrelated human and organisational benefits extending far beyond successful management of risk intelligence itself. Indeed, the notion that better risk intelligence management may lead to better, more confident and more engaged management in general, is one that we think contributes substantially to our case for formulating risk intelligence production as a simplifying managerial dexterity in the first place.

Now that all the above theoretical preliminaries have been attended to, we can begin to work through the range of matters which we think managers need to consider if they are to handle risk intelligence effectively. We start in the next section by exploring what an understanding of *intelligence cycles* can bring to the table.

INTELLIGENCE CYCLES

The *intelligence cycle* has been theorised into distinct phases in a multitude of ways to suit very different military, law enforcement and corporate purposes over the years. These also reveal some clear affinities with a number of information management processes which don't use the term *intelligence* at all. Table one provides a selection of these processes as follows:

Process Name	Simplified Chronological Sequencing						
Process Theory [(2011) MoD Joint Doctrine Publication 2-00]	Input	Transformation			Output		Outcome
Military Intelligence Cycle [(2011) MoD Joint Doctrine Publication 2-00]	Direction and Collection	Processing			Dissemination	Action	Continuous Review
Risk Management Process [(2018) ISO 31000]	Establish scope, context and criteria for risk management	Risk Identification	Risk Analysis	Risk Evaluation	Risk Treatment		Record, Report, Communicate, Consult, Monitor, Review
Change and Issue Management Process [(2013) PRINCE2 Projects in controlled environments]		Capture	Examine, Propose, Decide		Implement		Project Board/ Change Authority Daily Log/ Issue Register
Creating Market Insight [(2008) Smith & Raspin	Allocate Scanning Capability Responsibility, Reflect on Strategy, State Scanning Goals, Prioritise environment sectors for attention, determine scanning mix, assess market context, refine scanning mix	Contextualise information into knowledge	Select market insight from knowledge: is the knowledge valuable, rare, inimitable and organisationally aligned?		Implement		Assess probabilities of outcomes using marketing due diligence
Cloutier's (2013) Consolidated Competitive Intelligence Process	Planning, direction and collection	Analysis			communication	decision	evaluation
Criminal Intelligence Service Canada (2007): The Warning Intelligence Cycle	Threat Perception: Environmental scanning and scenario development		Evaluation and Monitoring: topic selection, indications research, threat/risk evaluation		Assessment and Warning: indicator list development, targeted collection, in-depth analysis, warning judgment		

Table 1: A Selection of Information Processes

Our primary purpose in setting out the above table is to urge Project Managers to consider that the best way to release project value from information may well be to give at least some regard to the thinking underlying *all* the above processes. The key question arising then is, what might an understanding of each process contribute to managerial dexterity for risk intelligence production? Working down through the rows, some key answers are, we think, as follows.

Firstly, process theory (referenced on the top row) alerts us to the importance of structured and phased management processes which extend beyond *outputs* to also encompass *outcomes* which may themselves require monitoring, analysis, periodic review etc. Essentially what this adds is an opportunity to consider each narrow output within broader and longer term management contexts. When this thinking is applied to information management it reminds us that reflection upon management usage of information might itself very productively stimulate and direct some further information search. This might in turn focus the mind on advantages that can arise from conceiving of information management effort as running iteratively and in cycles. Moreover, focusing on *outcomes* beyond *outputs* provides an opportunity to bring to bear a longer term information management concern with various organisational learning issues such as use of training events and effective documentation to retain and transfer knowledge, as well as retention of the intelligence skills that have proven useful in creating the knowledge. It further provides an opportunity to reflect on various intelligence *source* issues such as their reliability, the credibility of the intelligence they have provided, and effective ways to retain and develop them for further use.

Taking the next two rows together, what emerges in particular from the juxtaposition of widely used military intelligence and traditional risk management processes (or, more fully, *cycles*) is a particular *learning from military intelligence* issue. That issue is straightforwardly that traditional risk management processes can be enhanced by incorporating the military intelligence cycle's distinct *direction* and *collection* phases, essentially through targeted and proactive intelligence work. That can help address a particular problem, perhaps best summed up as the problem of risk identification effort often being too *sedentary* and reliant on existing management information. Arguably, the incorporation of direction and collection phases can help risk management become more *proactive* and *exploratory* right across the internal and external contexts of the project or organisation.

Following that, the inclusion of the fourth row dealing with change and issue management on projects, reminds us of the commonplace need to push information through structured information processes with urgency, where this may have direct and immediate implications for operational management. This may raise questions of what process to follow under time pressure, and in particular of alignment between various information management process to the change and issue management process. Getting this right, it may well be argued, can hold the key to *agile* project management.

Then on row five we have the insight creation process that is today widely associated with the marketing function. We have already referred to this as offering not just a form of words but perhaps also a distinct process for producing risk intelligence in its opportunity aspect. We think there is much advantage in seeking risk intelligence which is, as this process stipulates, *valuable*, *rare*, *inimitable* and *organisationally aligned*, such that its use can lead to sustained strategic competitive advantage. However, we also see no reason why the development of *insight* cannot be geared towards many types of lesser gain below the level of strategic impact.

The notion of a consolidated competitive intelligence process, mentioned on row six, references a very useful paper by Cloutier (2013). This paper draws attention to the long history, within management academia, of proposals for processes which continuously and systematically scan the business environment in order to deal with both opportunity and threat, and deliver strategic competitive advantage. It points out that such process proposals have gone by many names, including *environmental scanning, business intelligence, strategic intelligence, competitor analysis, competitive technical intelligence, market intelligence, peripheral vision* and *competitive analytics*. Indeed students of risk management may discern a clear overlap with the idea of the *corporate nervous system* that is sometimes considered to lie at the heart of *enterprise risk management* systems. Cloutier's conclusion, favouring a consolidated process solution based on the intelligence cycle, is arguably of interest for various reasons. Considered as a distillation of essential elements from diverse information management processes, there seems to be a good argument for using it widely.

Turning to row seven, it feels like pushing at an open – and very oddly, untraveled through – door, to suggest that risk management should make more use of the *warning intelligence* cycle mentioned there. Here it is interesting to see that both environmental scanning and scenario exercises are deemed important for generating key topics upon which warning analyses, the maintenance of warning indicators, and associated warning messaging, are to be based.

Looking at the table in overview, then, it becomes clear from this short selection of processes that risk intelligence production can very usefully be theorised as geared towards a number of possible ends. It may seek to anticipate risk (following the military intelligence logic of direction-collection) and to build resilience against the unexpected (through thorough use of environmental scanning). It can also gear towards insight creation, strategic decision-making, urgent implementation of changes to operational management, or indeed maintenance of warning indicators. From this there arises the following general discussion point:

Discussion Point 6: Managerial dexterity in risk intelligence production can usefully be viewed, in part at least, as an attunement to all of the above possible uses of risk intelligence information.

Our view is that any new encounter with risk information on a project, or within an organisation, can provide an opportunity to very briefly give some regard to all of these various possible reasons, and associated processes, for managing it. Arguably, issues are too often managed with a narrow instrumental rationality and a singular end in mind. Professionalism in risk intelligence can help to counter this problem, at least where new risk information is on the table for discussion, and where there is flexibility on ways forward for dealing with it.

To conclude, in the above discussion there is one vital process which we recognise we have neglected: that of the knowledge management process which raises data to become information, and information to become knowledge, and which carefully nuances different forms of knowledge. As we will soon concern ourselves with what it can mean to develop *risk knowledge* in particular, we will need to make some preliminary points about knowledge management in general. Before that, however, we dedicate the next section to exploring professionalised risk intelligence work in its aspect of evaluating the information upon which risk knowledge is always based.

INFORMATION EVALUATION: LEARNING FROM NATO

Looking back at rows two and three (in table one), where a military intelligence cycle and a traditional risk management cycle are juxtaposed, it becomes interesting to explore *learning from military intelligence* opportunities for the further advancement of best practice in risk management. One simple and yet highly valuable learning pathway is as follows. In military intelligence, and likewise in its various corporate adaptations, intelligence information is evaluated by rating both the *credibility* of the information and the *reliability* of its source(s). Traditional risk management processes, by contrast, require probability and consequence ratings for risks, but are altogether mute on matters of credibility and reliability for the information upon which risk ratings are based.

Arguably, risk professionals, and especially those who must deal with new risk information in real time on projects, should be making formal provision for credibility and source reliability evaluation in their discussions of risk information, at least to the extent that circumstances allow. Indeed, it could even be argued that project risk management is by necessity *always* project risk intelligence management, simply because there is *always* a plain advantage in undertaking at least some intelligence information evaluation whenever new information becomes available. Common sense dictates that new information will always be evaluated for credibility and source reliability, at least to some extent, by experienced professionals. And yet such evaluations may often remain vague, underarticulated and underdiscussed. There seems to be a clear case for transforming such practice by taking advantage of the structure and focus provided by formal use of a rating system. What's more, there need be very little additional time cost involved.

The routine use of credibility and source reliability rating systems, it can be argued, is viable and worthwhile under many stressful project circumstances. What's more this may often allow project managers to be seen to be taking as *professional* an approach as is possible to maintain under hectic circumstances. This may offer some worthwhile protection, both against unfair performance appraisal and against the *information fatigue syndrome* we mentioned earlier.

Fortunately, for Project Managers seeking such professionalism, military ratings systems can easily be carried over into project management use. Present day NATO intelligence doctrine advocates use of information evaluation criteria taken from the *Admiralty Code* originally designed in the 1940s by the Royal Navy. This comprises simple *reliability of information source* and *credibility of information* ratings. One of several recent and more detailed variants of this ratings system can be found in the (2003) STANAG 2511 report produced by the NATO Standardization Office. This is reproduced from Irwin & Mandel (2019) and set out below in tables 2 and 3 below:

A	Completely Reliable	Refers to a tried and trusted source which can be depended upon with confidence.
B	Usually Reliable	Refers to a source which has been successful in the past but for which there is still some element of doubt in a particular case.
C	Fairly Reliable	Refers to a source which has occasionally been used in the past and upon which some degree of confidence can be based.
D	Not Usually Reliable	Refers to a source which has been used in the past but has proved more often than not unreliable.
E	Unreliable	Refers to a source which has been used in the past and has proved unworthy of any confidence.
F	Reliability cannot be judged	Refers to a source which has not been used in the past.

Table 2: Reliability of Source (reproduced from Irwin & Mandel (2019))

1	Confirmed by other sources	If it can be stated with certainty that the reported information originates from another source than the already existing information on the same subject, it is classified as 'confirmed by other sources' and is rated '1'.
2	Probably true	If the independence of the source of any item or information cannot be guaranteed, but if, from the quantity and quality of previous reports its likelihood is nevertheless regarded as sufficiently established, then the information should be classified as 'probably true' and given a rating of '2'.
3	Possibly true	If, despite there being insufficient confirmation to establish any higher degree of likelihood, a freshly reported item of information does not conflict with the previously reported behaviour pattern of the target, the item may be classified as 'possibly true' and given a rating of '3'.
4	Doubtful	An item of information which tends to conflict with the previously reported or established behaviour pattern of an intelligence target should be classified as 'doubtful' and given a rating of '4'.
5	Improbable	An item of information which positively contradicts previously reported information or conflicts with the established behaviour pattern of an intelligence target in a marked degree should be classified as 'improbable' and given a rating of '5'.
6	Truth cannot be judged	Any freshly reported item of information which provides no basis for comparison with any known behaviour pattern of a target must be classified as 'truth cannot be judged' and given a rating of '6'. Such a rating should be given only when the accurate use of higher rating is impossible.

Table 3: Credibility of Information (reproduced from Irwin & Mandel (2019))

Such references to 'targets' and 'agents' may not always translate well into project contexts. Nonetheless, we think the above ratings system provides a useful basis for information evaluation on projects where information may be derived from many different sources.

Critical literature on variants of the Admiralty code emphasises that their ratings are intrinsically subjective. Irwin & Mandel (2019) suggest that making provision for collaboration and re-evaluation of the ratings, and for numeric probabilistic estimates of information accuracy (and perhaps for related confidence intervals) may be beneficial. Here it becomes particularly interesting to reflect on what risk professionals can bring to the table. Consider for example that the soft psychological and cultural skillsets of risk professionals will of often manifest as a concern to draw attention to false certainty – as indeed may be underlie a credibility rating of 5 where new information is rejected simply because it does not conform to a pre-existing pattern.

The discussion point to conclude this section is straightforwardly this:

Discussion Point 7: Use of credibility and source reliability ratings for information evaluation should be routine for project risk managers and risk professionals more generally.

KNOWLEDGE MANAGEMENT

For the remainder of this document we focus on the flow of information to become knowledge, and on how our understanding of knowledge can be nuanced to permit us to develop knowledge at higher levels of complexity. In other words, it is to knowledge management that we now turn, in order to explore what professionalism in risk intelligence production can entail.

Here we begin by looking at knowledge management literature in general. Much academic and practitioner literature links knowledge management (KM) to building effective information technology (IT) systems. Hence it often uses the terms *information* and *knowledge* interchangeably. Based on KM principles, firms have developed and implemented KM initiatives to increase the efficiency of business processes and productivity of their services, often with an IT focus. Moreover, innovation and sustainable competitive advantage (SCA) have been linked closely together and seen as a direct outcome of KM initiatives. This has sometimes resulted in traditional management models viewing firms as information processing machines, whereby problem solving is centred on what is inputted to the firm, and not what is thereafter developed and more broadly *managed* within.

Adopting the latter focus, we see risk intelligence production as very much concerned with ongoing risk knowledge development on a project, or within an organisation. Risk stories are, after all, things that may take shape slowly, following the pace at which pertinent information, such as loss data, becomes available. Moreover, we also think we can very usefully view risk knowledge as not exclusively bound up in clearly articulated risk stories. Sometimes it will manifest as behavioural ways of coping with risk, for example in applications of intuitive professional judgment (often involving use of *heuristics*) or of craft-like knowledge (sometimes called *techne*). Such ways of coping can be viewed as constituting valuable risk knowledge that may be slowly learned-by-doing while perhaps resisting the clear articulation that would permit the knowledge to be communicated more effectively.

Accordingly, we think Nonaka's (1994) idea of *knowledge conversion* from one distinct form to another, e.g. from *tacit* to *explicit* knowledge, can provide a very important conceptual framework for theorising the different forms and ongoing development (or *conversion* from one form to another) of risk knowledge. Knowledge management literature has much to say about the importance of *tacit knowledge* in particular, and we think it makes good sense to draw on it here. The knowledge based view (KBV) of the firm has long recognised individual repositories and social distributions of tacit and explicit knowledge as resources that need to be carefully understood and harnessed to deliver competitive advantage.

Georg von Krogh (1998) identified two major perspectives on the nature of knowledge. The revolution in computer science, systems theory, and neuroscience in the early 1950s, together underpin what is today called the *cognitivist perspective*. From this perspective, knowledge is universal, and the key task of the brain or any form of cognitive system is to represent or model a number of objects or events as accurately as possible. Hence, two cognitive systems should represent the same object or event, meaning that knowledge from the cognitivist point of view is able to be encoded and stored, is explicit, and is easy to transmit. By contrast, what Krogh calls the opposing *constructionist perspective*, views cognition as an act of construction or creation rather than representation. Hence, the cognitive system works when knowledge brings effective action. Krogh (1998) argues that knowledge is not universal and that knowledge resides within individuals who have senses and previous experience, hence, making individual experience and mental modelling of the world unique. The key point arising here is that tacit knowledge is by its nature something that is hard to express and share. We can view tacit risk knowledge in similar terms as an intuitive awareness and behavioural attunement to risk that is not readily expressed in the *risk stories* we referred to earlier. Moreover, we can regard it as potentially valuable knowledge that might easily go unrecognised within formal risk management processes that categorise and label risks.

The knowledge-based literature (e.g. Nonaka, 1994) almost always regards the organisational knowledge creation process as a dialogue between explicit and tacit knowledge. Taking stock, it becomes fascinating to further consider that on every project and in every organisation there is likely to be dialogue and perhaps tension between the social distributions of explicit and tacit risk knowledge present. Hence we might ask the following:

Discussion Point 7: Much of the risk that gets managed on projects can be considered tacit in character. Managers steer through the risk environment through the frequent exercise of professional judgment and technical proficiency, where, in effect, they access valuable tacit risk knowledge. This needs to be recognised within project risk management practice.

This point about technical proficiency, we think, merits some further clarification. After Nonaka the second most cited knowledge management author is Michael Polanyi. Polanyi (1958) does not make the strong claim that tacit knowledge cannot be transferred. Rather he suggests that some types of knowledge may be less amenable to transference than others. Hence, tacitness could be described as something personal such as a skill or ability to perform something or to resolve a problem that could be based on the individual's experiences and learning. He argues that with the appropriate use of language, some, but probably not always all, of this knowledge might be shared between individuals who share a mutually agreed language and meaning. Any predominantly tacit knowledge base is classified by Polanyi as "ineffable" to the extent that this problem of tacit knowledge transfer emerges. For example, ask Ronaldo how he hits the ball on a free kick and most people will probably not find his response helpful – and yet some professional footballers might make something of it. Ask a professional racing driver how they stay safe at high speed and it will probably be another racing driver who understands most of the explanation provided. Such explanations may be expressed most effectively through some combination of tone of voice, verbal and bodily communication. The implications for how we might further theorise tacit risk knowledge are fascinating. One way forward would be to accentuate the need to respect experienced professional judgments and associated dialogues at each stage of a risk management process, perhaps treating these things more explicitly as a valuable resource.

THE KNOWLEDGE CHALLENGE

"As projects become more global, computer systems more integrated and complex and infrastructure projects ever larger, we need to be smarter at how we learn from others' experiences. This is where Risk Intelligence has a crucial role to play in helping Project Sponsors to quickly identify the major technical and commercial risks that may impact their programme - and which often require holistic mitigation strategies, spanning wide geography and cultural diversity."

Stan Symons
Chairman of Wessex Branch (UK)
Association for Project Management.

DATA-INFORMATION-KNOWLEDGE CONVERSION

In order to more fully understand the nature and scope of risk knowledge, it can be helpful to consider some knowledge management perspectives on what makes knowledge differ from information. As Nonaka (1994, p.15) put it, *"information is a flow of messages, while knowledge is created and organized by the very flow of information, anchored on the commitment and belief of its holder"*. Based on this view, it may be helpful to regard risk information as something that is raised up, or *converted* to become, risk knowledge, at the discretion of the message recipient who has at least *some* possible action and usage in mind as a basis for valuing the information. Furthermore, the notion that information becomes knowledge through its organisation, reminds us of the importance of organising risk information within the structural elements of *risk stories*, as was discussed earlier.

More fully, however, the table below extracted from Stenmark (2002) provides some further points of differentiation to help us understand how *data* can be considered to become *information*, and how *information* can then be considered to become *knowledge*:

Author(s)	Data	Information	Knowledge
Wiig	-	Facts organised to describe a situation or condition	Truths and beliefs, perspectives and concepts, judgments and expectations, methodologies and know how
Nonaka and Takeuchi	-	A flow of meaningful messages	Commitments and beliefs created from these messages
Spek and Spijkervet	Not yet interpreted symbols	Data with meaning	The ability to assign meaning
Davenport	Simple observations	Data with relevance and purpose	Valuable information from the human mind
Davenport and Prusak	A set of descrete facts	A message meant to change the receiver's prospection	Experiences, values, insights, and contextual information
Quigley and Debons	Text that does not answer questions to a particular problem	Text does answers the questions who, when, what, or where	Text does answers the questions why and how
Choo *et al*	Tacts and messages	Data vested with meaning	Justified, true beliefs

Table 4: Data, Information and knowledge (from Stenmark (2002))

It is noteworthy that these various perspectives, taken together, invite a subtle view of risk knowledge, recognising both *explicit* risk stories and more *tacit/ineffable* knowledge manifest within behavioural ways of coping with risk. It is the blend of the two, we suggest with reference back to the discussion in the last section, that can often matter most. More fully, we might infer from the knowledge column in table 4 that risk knowledge might conceivably, on occasion, require to be understood as subtly aligned across multiple forms listed there.

Earlier we suggested that explicit and tacit knowledge will always tend to contain elements of each other. To now expand on that observation, the flow of data-to-information-to-knowledge can be viewed as a continuum where knowledge complexity increases with tacitness. Figure one (below) is adopted from Ceylan (2018) to illustrate our point:

Figure 1: Complexity of Knowledge Diagram (From Ceylan, 2020)

In this diagram, low complexity knowledge is also assumed to be relatively explicit and therefore easily transferable. This is where we are likely to find our most simple risk stories. As we move into relatively tacit and highly tacit knowledge domains, knowledge complexity increases as its highly tacit and therefore less easily transferrable elements come to predominate. This is where, we suggest, risk knowledge is more likely to exist, subtly aligned in multiple forms, as we explained above.

Next we look closer at knowledge production pitched at higher levels of knowledge complexity. Nonaka and Takeuchi (1995) argue in their knowledge conversion model that an organisation creates new knowledge through the interaction between tacit and explicit knowledge. Their resulting four modes of knowledge conversion are as follows:

(1) Socialisation – from tacit knowledge to tacit knowledge.

(2) Internalisation – from explicit knowledge to tacit knowledge

(3) Externalisation – from tacit knowledge to explicit knowledge

(4) Combination – from explicit knowledge to explicit knowledge.

These four concepts, we think, get us closer to understanding risk knowledge production on projects and in organisations. Essentially they help us to conceive of risk knowledge as something dynamic, and not just as existing in multiple forms but also as shifting in form through daily management interaction. For *socialisation*, consider the importance of on-the-job training for communicating behavioural strategies that cope with risk. For *internalisation*, consider the importance of learning from verbal and visual representations of risk by resolving these down into behavioural strategies. For *externalisation*, consider the importance of providing verbal assurance on the effectiveness of behavioural strategies, as well as the need to codify these as clearly as possible for organisation learning purposes. For *combination*, consider the importance of restating risk knowledge within the language favoured by, and indeed most useful to, some target group; for example the conversion of risk discourse into the language of finance for boardroom discussion is a widely recognised practice.

Consider also, that for each of these four modes of conversion, it is not just risk *communication* that is taking place; rather, there is a meeting of minds where separate experiences, intelligences, stocks of knowledge and risk perceptions collide, thereby creating the conditions for new risk knowledge to come into existence. A discussion point arises here as follows:

Discussion Point 8: The four modes of knowledge conversion highlight four important pathways for communicating, improving and applying risk knowledge through interaction between project participants.

CONCRETE AND ABSTRACT RISK KNOWLEDGE

Next, we theorise risk knowledge as taking two basic forms: *concrete* and *abstract*. When we have some information about a possible risk, this may be rendered as risk knowledge within some abstract specification of a particular risk category. Hence we would say *this sort of risk may happen here*. Alternatively, risk information may be rendered as risk knowledge within some *concrete* specification of what is actually happening, based on actual experience of it within some project or organisational environment. The difference may seem subtle at first, but we believe the importance of recognising it can be tremendous, from an Intelligence production, coordination and decision-making point of view.

At this point, we would like to reintroduce the 'Complexity of Knowledge Diagram' to reflect our suggestion of a general tendency for risk knowledge to grow ever more *tacit* and *abstract* at higher levels of risk knowledge complexity. Our thinking here is as risk knowledge grows more complex and becomes more integrated within behavioural ways of coping, prospects for verbal representation in the simplified management language of risk are likely to diminish. This means risk knowledge will increasingly be expressed in the form of abstract categories; that is, with reference to the theoretical spaces where complex risk knowledge can usefully be situated or contextualised in various respects. Consider, for example, that many high level risk categories such as operational risk or reputational risk simply establish a theoretical space in terms of what is *exposed* to risk. They allow complex risk to be acknowledged and discussed in outline, not described in detail. We express this idea in figure 2 below:

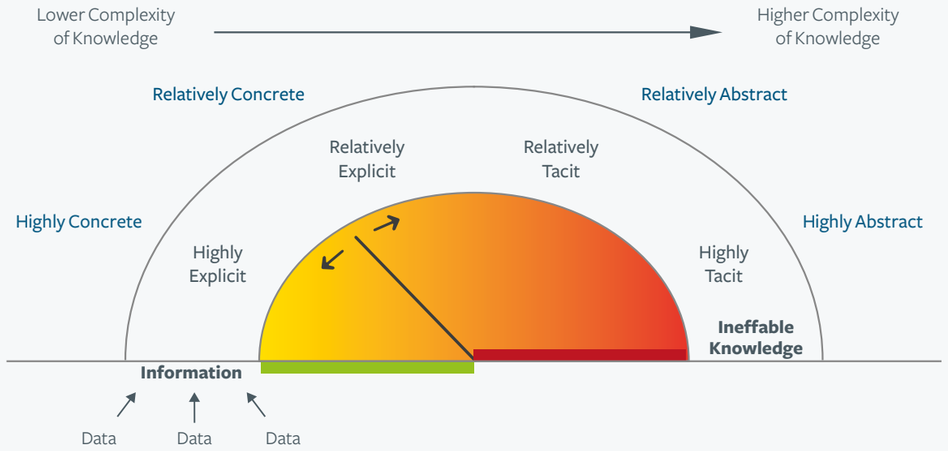


Figure 2: Complexity of Knowledge Diagram (From Ceylan, 2020)

The extent to which we prefer to focus on concrete or abstract risk knowledge might usefully be considered as a question of which *mind style* we prioritise, perhaps as an acquired management habit, in order to learn about what is going on in the world. Anthony F. Gregorc's (1984) *mind styles model* calls attention to a *concrete-sequential* mind style which has been a favourite for project managers for a long time, as illustrated by commonplace usage of waterfall methodologies to manage projects. Drawing on this, it can be argued that project managers need a *concrete* mindset focused carefully on the here-and-now of the *specific* conditions and challenges that confront them; just as importantly, they need a *sequential* mindset which thinks *causally*, linking elements in a linear fashion, in order to think through the best ways to move their projects towards desired performance outcomes amidst risk and uncertainty. That is essentially what concrete-sequential mind styles are all about. Clearly they are a bread-and-butter necessity for daily project management.

However, such views arguably struggle at higher levels of risk knowledge complexity. Sequential process models, such as waterfall methodology, are most effective when the problem is well defined, and the solution and risks are well understood. However, risks often require to be *theorised* in exercises of the risk imagination where what matters most is an *abstract* view of the world which learns *isomorphically* by modelling present risk exposures on previous risk experiences that might have happened *anywhere*, and to *anyone*, under at least partially similar circumstances. Hence abstract mind styles, and dare we say it, Gregorc's *abstract-random* mind styles, arguably deserve more recognition within project risk management. We think there is an issue of psychological dexterity here, best expressed as a discussion point as follows:

Discussion Point 9: Professional competence in handling risk intelligence, surely, requires and understanding of how risk intelligence is *always* comprised of some combination of abstract and concrete risk knowledge.

Without the artistic mind's abstract-theoretical imagination, we suggest, risk imagination would be severely constrained, especially in its handling of novel or unusual risk. The more complex the project environment, the more difficult it becomes to resolve that complexity within a risk narrative that is viable for practical management purposes and the more important mind style diversity, switching, balancing, etc., become.

FOUR STATES OF RISK KNOWLEDGE

In this penultimate section we highlight one last *learning from military intelligence* issue which we think is very relevant for scrutinising and developing risk knowledge at higher levels of complexity. The four military intelligence expressions, *known-knowns, known-unknowns, unknown-knowns,* and *unknown-unknowns* have become well known following a (2002) speech on weapons intelligence by (then) US Secretary of Defense Donald Rumsfeld. According to Marshall et. al (2019), these expressions can be interpreted as referring to differing levels of abstract and concrete risk knowledge as follows:

Known Knowns High level of abstract risk knowledge High level of concrete risk knowledge	**Unknown Knowns** Low level of abstract risk knowledge High level of concrete risk knowledge
Known Unknowns High level of abstract risk knowledge Low level of concrete risk knowledge	**Unknown Unknowns** Low level of abstract risk knowledge Low level of concrete risk knowledge

Figure 3: Four states of Risk Knowledge (adapted from Marshall et al., 2019).

On this view, *unknown unknowns* can describe circumstances where both abstract theoretical imagination and environmental scanning for weak signals have little to offer. Then there are *known unknowns* where the risks at issue are discussed notably more in terms of abstract theory than with reference to actual evidence and, conversely, *unknown knowns* where there are perhaps confluences of weak signals threatening disruption, and yet abstract theory struggles to capture these within its preferred risk category designations. As the epistemic capstone on top of all this there are *known knowns* where risks are well understood, both theoretically and in terms of actual impacts. These will often be *insurable* high frequency low impact risks.

We suggest that the current state of knowledge for any given project risk can be evaluated by applying each of these four theoretical prisms to see how well they fit. Clarifying *unknown unknowns*, aside from helping to root out false confidence and false assumptions, can help support deliberation about competitive differentiation in terms of appetite for dealing with uncertainty. To gather more evidence for a *known unknown*, or to spend time on theoretical contexualisation for *unknown-knowns*, might be understood as purposeful engagement in the epistemic enterprise of converting or raising all risks to become *known-knowns*. However, at this point it is interesting to return to our knowledge complexity diagram one last time in order to consider how such purposeful activity may be frustrated at higher levels of knowledge complexity.

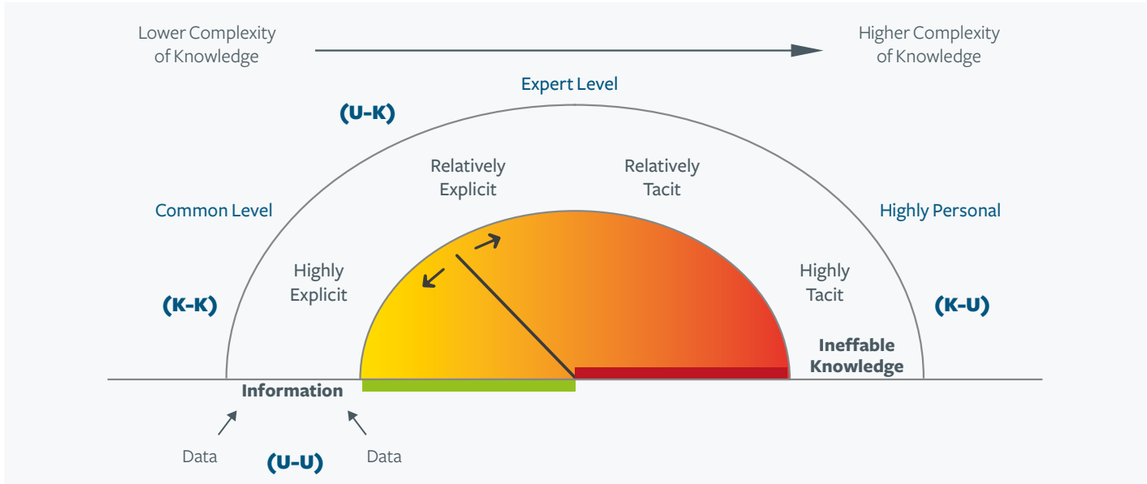


Figure 4: Complexity VS Four States of Risk Knowledge

Our conclusion, then, can be summed up as follows:

Discussion Point 10: A mature approach to risk intelligence production entails not just the pursuit of *known-knowns* but also a recognition that managerial distributions of *known-unknown risk* may require to be recognised and cultivated for their perhaps often undervalued contributions to project success.

FINAL CONCLUSION

We hope that this document has provided some helpful insight into what *producing risk intelligence* can mean. Fundamentally, our concern has been to collide various ideas and practices from project management, risk management, knowledge management and intelligence management, to produce a critical mass of new ideas. We have bundled these new ideas together under our risk intelligence heading. However, there is no reason why readers should not value each of them separately. And we hope that readers will have cause to value and make use of at least some of them.

All that remains is to invite feedback from Professionals in Project Management and related disciplines, regarding whether and to what extent our suggestions seem helpful. Any feedback suggestions on how to further develop the theory or practice of *risk intelligence production* are particularly welcome.

BIBLIOGRAPHY

Axelos. (2017). Managing Successful Projects with PRINCE2. Sixth Edition.

Ceylan, S. (2020). AgileFrame: Understanding multifaceted project approaches for successful project management. IPMC Publishing.

Cloutier, A. (2013). Competitive Intelligence Process Integrative Model based on a Scoping Review of the Literature. International Journal of Strategic Management, 13(1), 57-72.

Criminal Intelligence Service Canada (CISC). (2007). "Strategic Early Warning for Criminal Intelligence: theoretical framework and Sentinel Methodology".

Gregorc, A.F. (1984). "Gregorc Style Delineator: development, technical and administration manual. Gregorc Associates, Inc.

International Organization for Standardization (ISO). (2018). "Risk Management – Guidelines".

Irwin, D. & Mandel, D.R. (2019). Improving Information Evaluation for Intelligence Production. Intelligence & National Security. Available online February 2019.

von Krogh, G. (1998). Care in Knowledge Creation, California Management Review, 40(3), 133-153.

Marshall, A., Johnson, J. (Ed.), Dawson, I. (Ed.), Lin, F. (Ed.), & MaCrae, C. (Ed.) (2017). "Risk Intelligence: a Centre for Risk Research discussion document". University of Southampton.

Marshall, A., Ojiako, U., Wang, V., Lin, F. & Chipulu, M. (2019). Forecasting Unknown-Unknowns by Boosting the Risk Radar within the Risk Intelligent Organisation, International Journal of Forecasting, 35(2), 644-658.

Ministry of Defence (MoD). (2011). "Joint Doctrine Publication 2-00".

NATO Standardization Office. (2003). STANAG 2511.

Nonaka, I. (1994). A Dynamic Theory of Organizational Knowledge Creation. Organization Science, 5(1), 14-37.

Nonaka, I. & Takeuchi, H. (1995). "The Knowledge-Creating Company: how Japanese companies create the dynamics of innovation". Oxford University Press.

Polanyi, M. (1958). "Personal Knowledge: towards a post-critical philosophy". Routledge.