Institute of Risk Management

Extended Enterprise:

Managing risk in complex 21st century organisations

Resources for practitioners

SureCloud

irm

Our supporters

Contents

Our project team

IRM would like to thank our own extended enterprise which has come together to draft and review this guidance. Those that took on the task of writing individual chapters and case study authors are also named against their sections.

Neil Allan SIRM, Systemic Consult Ltd & University of Bristol, UK
Richard Anderson FIRM, Anderson Risk, UK, IRM Chairman
Mike Bartlett FIRM, Network Rail, UK
Jeremy Bendall, Bendall Advisory, NZ
Darren Brooks, BAE Applied Intelligence, UK
Andy Bulgin FIRM, AB Risk Consulting, UK
Philip Coley CIRM, Zurich Risk Engineering, UK
Colette Dark MIRM, Gallagher Bassett, UK
Christos Ellinas, Systemic Consult Ltd & University of Bristol, UK
Depeche Elliot SIRM, Maclear SA
Dean Fathers, Cass Business School & Nottinghamshire Healthcare, UK
Steve Fowler FIRM, IRM, UK
Roger Garrini, IRM Affiliate, Selex ES, UK
Sarah Gordon CIRM, Satarla, UK and South Africa
Louise Gravina, IRM Affiliate, Sainsbury's, UK
Jeremy Harrison FIRM, IRM, UK
David E Hawkins, Institute for Collaborative Working, UK
Richard Hibbert, SureCloud, UK
Alex Hindson FIRM, Amlin AG, Switzerland
John Joyce SIRM, Allianz Insurance, UK
Patrick Kiryowa, IRM Student, Eskom Uganda
Mike Morley Fletcher, IRM Affiliate, ARC & Associates, UK
Peter Neville-Lewis MIRM, Principled Consulting, UK
Jeremy Philpott MIRM, Lloyd's Banking Group, UK
Dan Roberts SIRM, First Central Insurance Management, UK
Keith Smith FIRM, RiskCovered, UK, IRM Director
ManMohan Sodhi, Cass Business School, UK
Jake Storey, IRM Affiliate, Gearbulk, UK
Amelia Stubbs, IRM Affiliate, Korn Ferry Whitehead Mann, UK IRM Director
Colin Tester SIRM, AXA, UK
John Thirlwell, Institute of Operational Risk, UK
Steve Treece FIRM, Health & Social Care Information Centre, UK
Elliot Varnell, IRM Affiliate, Pension Insurance Corporation, UK
David Welbourn, Eutropia Ltd and Cass Business School (Visitor), UK
Nick Wildgoose, Zurich, UK
Carolyn Williams MIRM, IRM, UK

Thanks also to many others who have helped with resources, comments, references and support and who responded to our consultation documents.

Foreword

Each year the Institute of Risk Management (the IRM) undertakes a major study expanding the limits of understanding and consensus about risk management. Previously we have produced critically welcomed guidance on Risk Appetite and Tolerance, on Risk Culture and on Cyber Risk.

This time we are examining how we manage risk in today's complex organisations, their value chains and networks of relationships - what many call the 'extended enterprise'. We're looking at how all organisations are affected by the way that others in their value chain and network manage risk and the complexities that can arise from these relationships.

I am grateful to the IRM members and other experts (all named in this document) who came together to produce this work over the past 18 months. I would also like to thank the wider group of IRM members, practitioners and academics who have commented on the work, attended our workshops and otherwise supported the group.

Extended enterprise is about far more than 'supply chain risk management' (although that is an important component): we are looking beyond supply into the complex network of relationships that underpin public and private economic activity in modern economies. In fact our work grew to focus on the nature of complex 21st century organisations in a world of 'VUCA' (volatility, uncertainty, complexity and ambiguity) and how risk can be managed in that context. Outsourced services, IT security, supplier assessments, joint ventures and partnerships, alliances and informal arrangements, together with the speed of change can all present challenges. And management of risk in the value chain can only ever be as effective as the management of the weakest link in it. Likewise, concern about values and ethics needs to extend beyond the areas within the organisation's immediate control. Our study looks at how these issues interact and explores some tools and techniques that can help us understand and address the extended enterprise challenge.

This document - 'Resources for Practitioners' comprises a series of chapters written by different members of our project group. Some chapters provide academic analysis; others focus on highly practical applications and experience.

The group has also produced a shorter document which distils the contents of this detailed resource pack into an executive summary with a particular focus on the questions that boards, assisted by their risk professionals, should be asking about risk in their own extended enterprises. This executive summary is available for free download from IRM's website and those of its partner organisations for this project.

As with all our thought leadership work, we have tackled a new subject where practice is still being developed. We have suggestions to make, based on practitioner and academic input, but we don't believe this will be the last word on the subject - we expect to see new ideas emerging and welcome comments.

Thanks are also due to our very patient sponsors, SureCloud. As well as contributing their expertise to the content, their support has made possible the design and print of these documents. As a not for profit organisation, IRM is reliant on enlightened industry support like this to help us maximise our investment in the development and delivery of world-class education and professional development activities.

Richard Anderson, Chairman

SureCloud is proud to support this thought-provoking study which will provide risk professionals and executives with an appreciation of the risks posed by direct and arms-length trading relationships, and paves the way for effective management of these risks. Today, enterprises seeking to assess and manage their extensive network of suppliers, partners or associates are facing common challenges: who are their suppliers, which pose the greatest threat, where should effort be focused to minimise exposure to the organisation? This study delves deep, highlighting where risk may occur in the extended enterprise and proposes methodologies and tactics to secure the organisation whilst benefiting from the efficiencies they bring.

Richard Hibbert
CEO, SureCloud

Chapter1: Extended enterprise - an overview

Richard Anderson

Classic risk management, in line with much thinking about management as a whole, concentrates on the entity: an entity that acquires some capital, builds capability, employs people, delivers services, processes raw materials and sells its product to a consumer. Porter[1] developed the archetypal model for this in the form of his Five Forces model which analyses an industry or a participant by looking at the threat of new entrants or substitution, and the determinants of supplier and buyer power (see Figure 1.1).

Figure 1. 1: Porter's Five Forces model

Of course, in reality, we know that business is no longer like this: all businesses consist of a complicated network of entities that might include multiple-tiered supply chains, with sub-contracted manufacturing, licensed intellectual property, outsourced back offices and complicated routes to market, in essence what we are calling the extended enterprise.

Moreover, risk management is now normally practised with the fundamental flaw that risks are looked at in isolation within the organisation. Like economists, risk managers have a penchant for looking at any given risk ceteris paribus – everything else remaining constant. While some look at scenario planning, that probably remains a small minority in the ranks of risk managers. And yet we know perfectly well that if one thing goes wrong, it is quite possible, indeed probable that there will be a cascade of other issues, any number of which might go better or worse than expected had the first risk not "exploded". This failing can be even more severe when we look across the extended enterprise at risks that might actually go better than expected in a second tier supplier, but which then adversely affect us. It is our remains a small minority in the ranks of risk managers. And yet we know perfectly well that if one thing goes wrong, it is quite possible, indeed probable that there will be a cascade of other issues, any number of which might go better or worse than expected had the first risk not "exploded". This failing can be even more severe when we look across the extended enterprise at risks that might actually go better than expected in a second tier supplier, but which then adversely affect us. We suspect that while many management teams are still considering the colour status of their risk maps, we simply do not have the toolset in general usage to address these much more fundamental issues: how should we visualise (or map) our extended enterprise? Where are the key risk nodes? What do we need to go right outside of our control so that we can manage our own destinies?

A definition

Our definition of the extended enterprise is one in which a number of organisations come together in order to achieve some outcomes that none of them can achieve on their own, within the timescale within which they wish to operate, with the skills available to them.

For example, Rolls Royce uses Kidde Graviner (a small firm by comparison) because Kidde Graviner is the market leader in fire suppression. While Rolls Royce could have dealt with this in-house, they believed that the quality of Kidde Graviner's product and reputation in this field were of value in the overall joint endeavour of creating their aero-engines.

This concept can be shown diagrammatically as follows. Figure 1.2 shows a joint endeavour, probably based in multiple economies in diverse societies with many people and organisations trying to achieve certain outcomes, while Figure 1.3 shows the interconnections of some of the component parts of that joint endeavour.

1. Porter, M.E. (1980) Competitive Strategy, Free Press, New York, 1980

Figure 1.2
Joint Endeavour

Multiple Economies
in Diverse Societies

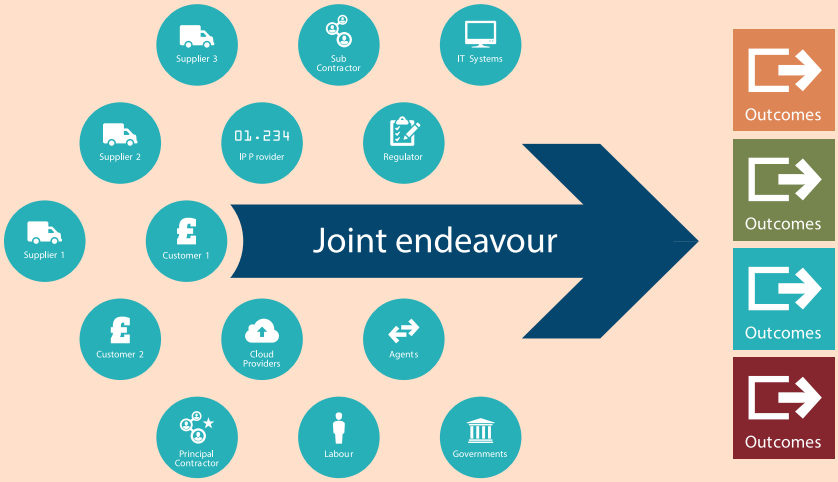
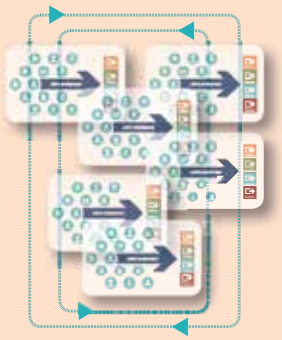
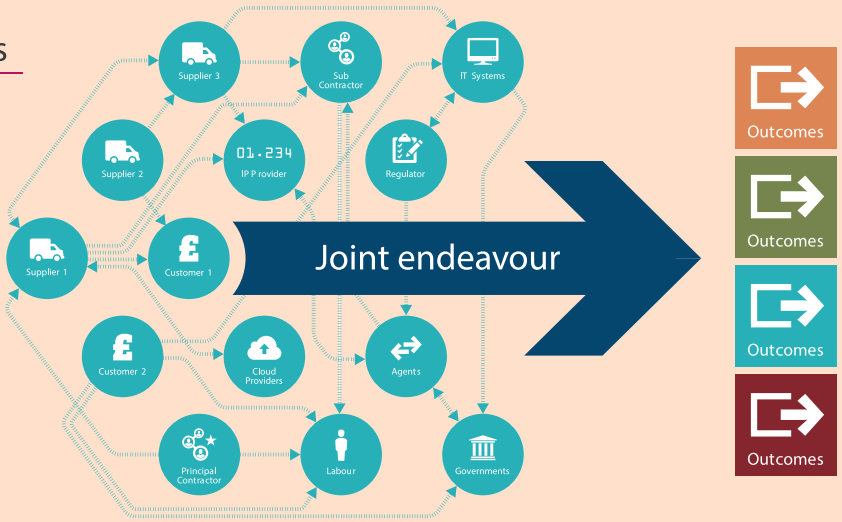


Figure 1.3
Further Interconnections

Multiple Economies
in Diverse Societies





We will all recognise projects, organisations and indeed whole industries that fit into this pictorial representation. The arrows show connectivity between different elements, and are merely illustrative, the point being that the picture is complicated.

In a traditional model of risk management, it is quite likely that some of the component parts will have good risk management within the bounds of their own organisations, while some will have poor or non-existent risk management. It is equally possible that some elements of the joint endeavour will share parts of the risk management equation: it is increasingly common that principals in the extended enterprise will exercise some form of "third party" risk management. However, what is absolutely clear is that the web of complexity means that any one party's risk management can only be as good as the weakest link.

Furthermore, regulatory and governmental influences and indeed societal expectations in many disparate economies will inevitably have differing, if not conflicting impacts on how different parts of the extended enterprise manage risk or indeed how they perceive risk (what is a risk in one country may not be perceived as a risk in another). But of course, even as we simplify the picture above, each of the participants is likely to be involved in multiple "extended enterprises", and the inter-relationships become even more convoluted:

It is within this overall context, that our work on this paper started by looking at the extended enterprise, but has grown to encompass complexity in the 21st Century Organisation. There are several reasons for this:

- Everyone that we have spoken to in the course of writing this paper has recognised that risk management is no longer an issue for single businesses. For years now risk professionals have been preaching, evangelising even, a concept of enterprise risk management that we all know is limited in its scope, because no business is any longer an island in the global economy. Some attempts at shoring up the concept have included a growing body of thinking about "supply chain" or "third party" risk management, but we all know that supply is only one element of the complicated web that now forms the overall business "ecology".

- Everyone is now conscious of information security (of course being conscious of it does not mean that everyone is doing it well), but information security risk is often treated as a specialism in its own right.

- As acknowledged by the movement towards integrated or sustainability accounting and reporting, we all know that we owe some sort of duty to a variety of stakeholders, and sometimes we have to provide them with messages that have some form of "assurance" statement (for example the annual report to the shareholders). But the bewildering complexity of who we need to provide these messages to in a complex world is far from clear.

- There are varying degrees of formality in the arrangements in any extended enterprise, some bound (or some parts bound) by legal arrangements, and some may be purely temporary fixes to deal with short term problems or to capitalise on short term opportunities. For example a typical mobile phone supply chain might only exist for twelve months while a particular model is available on the market.

And yet at the same time, it is ever clearer that traditional risk management programmes are struggling to keep up with modern business practices. The examples of risk management failures even since the Global Financial Crisis ("GFC") are legion:

- Phenylbutazone ("Bute") contaminated horsemeat, and a lot of other things, were identified in beef-labelled products destined for the human food chain;

- Banks around the world have mis-sold insurance and other products and manipulated key LIBOR interest rates;

- Failures to comply with Anti-Money Laundering ("AML") regulations in the US have resulted in eye-watering fines for French and British banks alike;

- Government suppliers are alleged to have invoiced for "tagging" dead people;

- The Chinese authorities are investigating corruption in the pharmaceutical industry.

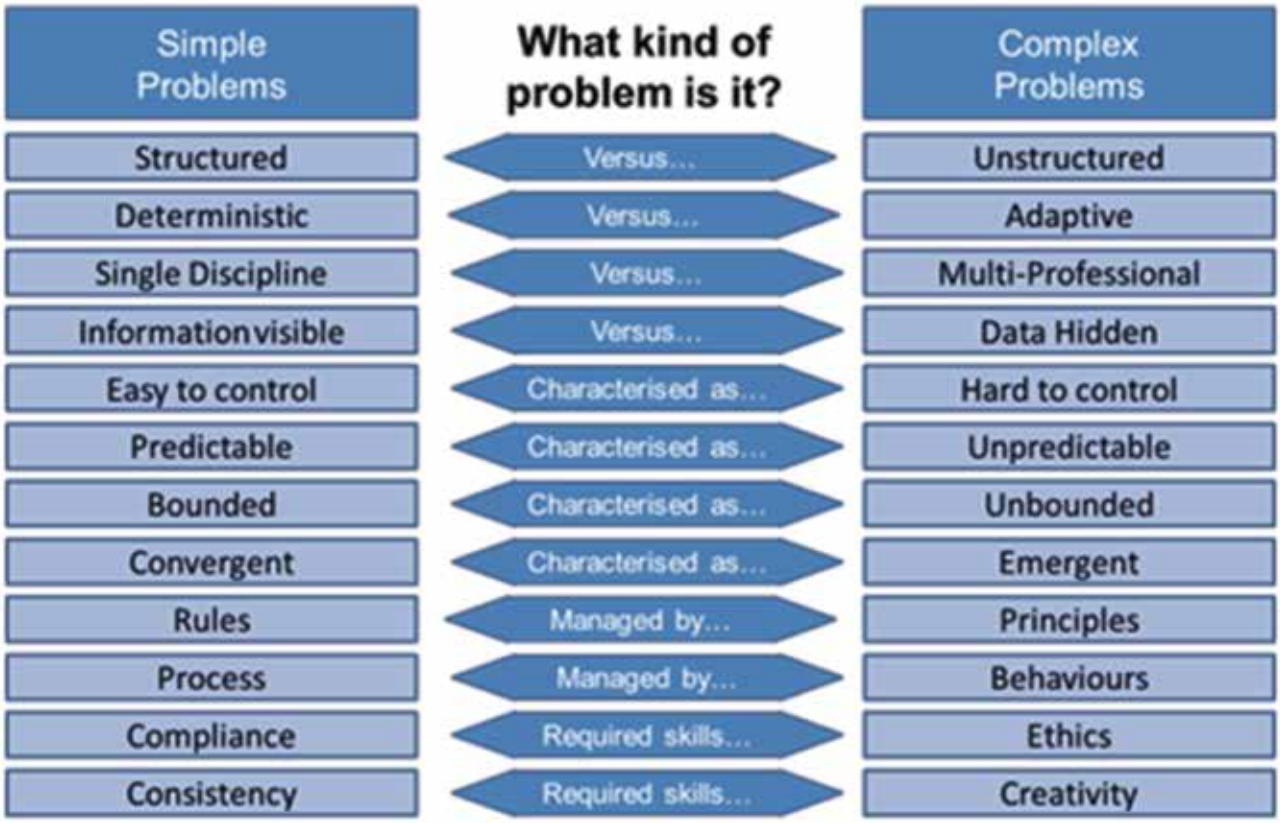
All of this in the context of businesses that in very many cases would claim to have fully implemented ERM programmes. So just what is going wrong? It may be that overly simplistic approaches to risk management are providing a degree of reassurance that simply is not warranted. Many commentators would argue that risk management is not complicated: after all, as set out in ISO31000 it is a matter of identifying, analysing, evaluating and treating the risks. Of course the first step in the ISO31000 process is establishing the context and it is precisely in that area that this work is focused.

Businesses are increasingly complex, and the risks that they face continue to evolve not simply in proportion to the complexity of the organisations themselves, but at a rate that is compounded by the complexity of the environment in which they operate. It is therefore incumbent on risk management professionals to help organisations to understand this complexity and to help hard-pressed management teams to navigate a path through the risks that they face.

Our starting premise for this paper is that risk pervades that very complexity, and therefore the enterprise risk management model can be of limited use, just because of that complex environment within which most organisations operate, whether they are publicly traded global organisations, government agencies, international not-for-profits or simple private companies: all of them face a complex environment. Our contention therefore, is that saying, as many have done, that risk management is a simple matter of identifying, assessing, recording and responding to risks is a simplification too far. While all of those things need to be done, they need to be done with a deep understanding of the complex environment.

In summary, we are living in a world of volatility, uncertainty, complexity and ambiguity: VUCA for short. We believe that living in this world, where there is chaos and therefore a forward vision of paradox (in other words we are unable to provide a logical analysis) we will be making sub-optimal decisions unless we can develop the risk management toolset to begin to understand the multiple futures that we all face.

Figure 1.4: What kind of problem is it?



So what do we mean by a Complex 21st Century Organisation? We have developed three simple tests to see whether traditional approaches are likely to work or not:

Test 1: is the problem simple or complex?

Test 2: are we dealing with a single enterprise in a sole endeavour or multiple organisations in a shared endeavour? and

Test 3: Is the span of control distributed amongst many participants in the shared endeavour?

Test 1 – Simple or complex

Our first test is to ascertain whether an organisation is dealing with simplicity or complexity. This is summarised in Figure 1.4 below, and looks at:

Four attributes of problems: these four attributes help to contrast simple and complex problems.

- A simple problem is one which is usually structured in the sense that we have seen similar issues, we know how to resolve them and they are susceptible to a fairly routine set of tasks. In contrast, complex problems are unstructured.
- Simple problems are deterministic in that if you do the right things to resolve the problem, then a predictable set of outcomes will arise. In contrast, complex problems are adaptive in the sense that as you carry out certain tasks, it is highly likely that new and unexpected problems will arise.
- Simple problems are normally susceptible to a single professional discipline, whereas complex problems often require multiple disciplines working together in ways that had not previously been imagined.
- wIn simple problems, much of the information that is required to manage the issue is easily available, whereas in complex problems, vast amounts of data may well be available, but finding the right bits of data can be like searching for a needle in a haystack.

Four characteristics of problems: simple problems are characterised as being easy to control, predictable, within a set of well-known and understood boundaries and typically convergent in that they will respond in an expected way leading us down a path towards resolution of the problem. In contrast, complex problems are by their nature hard to control, are unpredictable, have complicated or unknown (or even unknowable) boundaries and are emergent in so much as each step along the path will continue to throw up new and unexpected problems.

Two management approaches: typically simple problems can be dealt with by a set of rules and predetermined processes. In contrast, complex problems are likely to be managed by understanding a set of principles and expected behaviours which will help to determine the most appropriate route through the problem.

Two sets of different skills: These management approaches require starkly different skills. Rules and process are best managed by compliance and consistency (always doing the same thing) whereas principles and behaviours are underpinned by ethical values and almost always require creativity.

In looking at simple versus complex problems we run the risk of setting up binary choices which would mean that we are falling into the very trap we are seeking to avoid. However, by starting to understand the multi-layered nuances implied by this analysis we can start to think about where we are on the spectrum from simple to complex and that will help us as we decide which tools might be more beneficial in our management task.

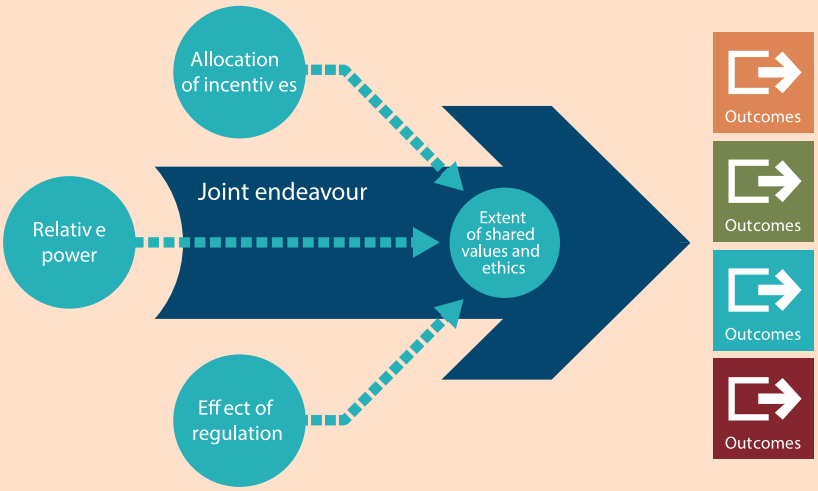
Test 2: single enterprise or multiple enterprises in joint endeavour

Our opening assumption is that most major objectives these days need multiple enterprises in order for the full range of resources to be brought to bear to the issue in hand: we illustrated that earlier in Figures 1.1 and 1.2. Whether it is building a space station in orbit (too big either for the Americans or the Russians on their own) or building a hydro-electric plant (too diverse a range of skills needed for most construction companies to do this on their own) or providing services to safeguard vulnerable children and adults in our society (where multiple agencies have specific roles to play), or simply bringing a new product to market, the likelihood is that multiple organisations will be required in order to achieve the desired outcomes.

We envisage this as set out in Figure 1.5 below. In essence a number of organisations agree to undertake a specific exercise, which requires all of their joint skills – a "joint

Figure 1.5
Key Dynamics

Multiple Economies in Diverse Societies



endeavour". The likelihood of successfully achieving the desired outcomes will depend on at least four elements:

Power: who has the power in the relationship? Is it shared or is it in the hands of one of the parties? The relative power of various participants may not necessarily be immediately obvious and needs some investigation.

Incentives: who is extracting value out of this endeavour for what? What are the monetary and non-monetary rewards? Do targets align to support the joint endeavour or are these in conflict with the potential to produce undesirable outcomes? How are the decisions made? What is the basis of allocating the reward?

Regulation: are there governmental, professional or industry regulations that are brought to bear on the subject in hand?

Values and ethics: is there a sense of shared values and ethics across the joint endeavour? Or is every participant only out for their own interests?

Again, it is worth emphasising that the extended enterprise is nothing new. What is new is that the speed of communication, the complexity and the sheer scope of these virtual organisations render any attempt to manage risk purely within the boundaries of one component of the extended enterprise a probable failure. The diagram set out above is a framework for understanding the scale of the issues that we might face.

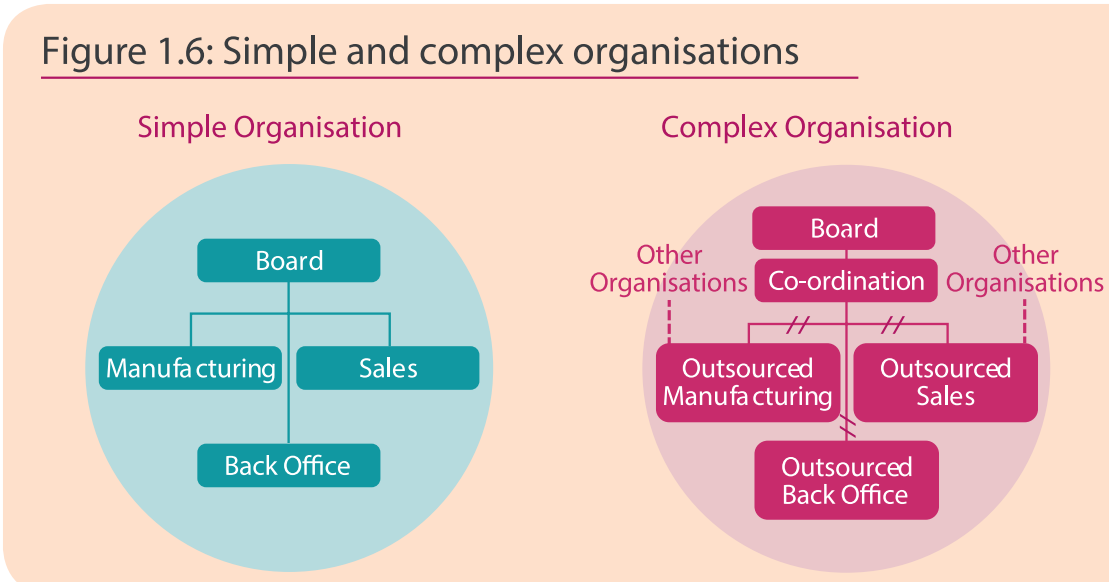
Test 3: the span of control

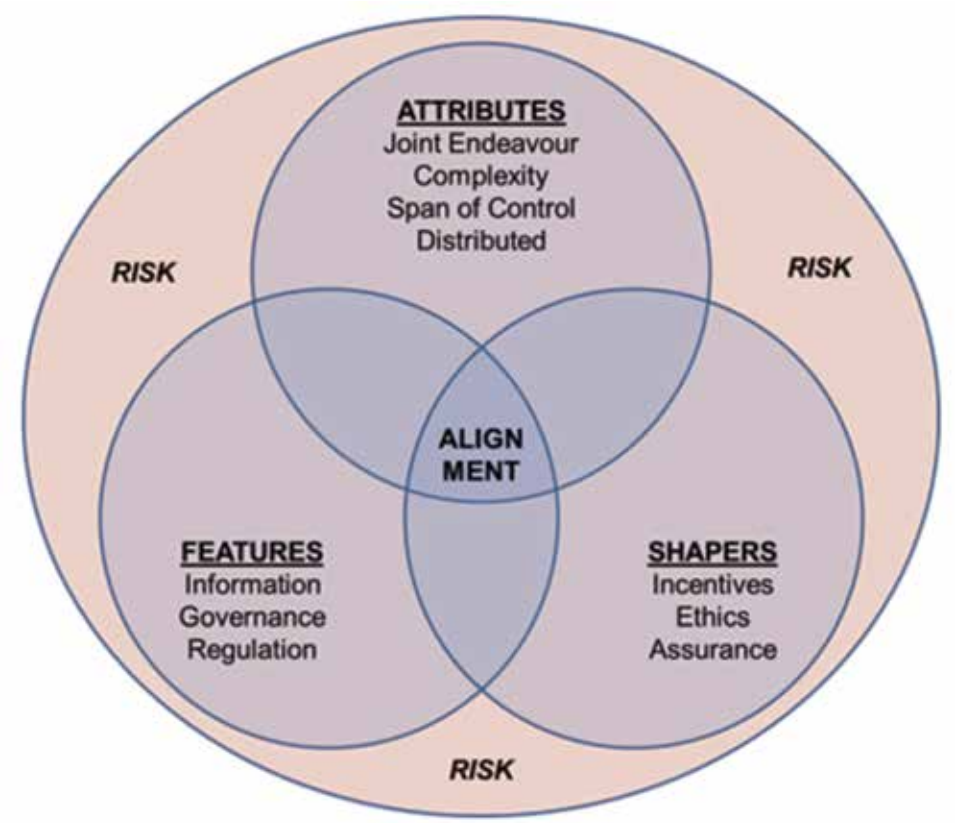
One of the essential pre-requisites of deciding whether or not we are dealing with an extended enterprise is the extent to which the span of control reaches outside of one organisation and into multiple other organisations. For example, where an organisation outsources its back office to an IT provider in India, and its manufacturing to China, while it uses sales agents in non-domestic markets and pays a licensing fee to the owner of some intellectual property, then we are dealing with an extended enterprise. This is shown diagrammatically in Figure 1.6 below:

In the simple organisation, the board controls the manufacturing, the sales and the back office, and communication of instructions and feedback is direct within the same span of control. In the complex organisation, or extended enterprise, the board has to have a co-ordination role because each of the manufacturing, sales and back office are outsourced to third parties. Many brand-based organisations operate in this manner, and indeed it is not uncommon for banks and other financial institutions to outsource many aspects of their businesses. The difficulty that this imposes is that the communication lines are broken as those that carry out the detailed activities of manufacturing, sales and the back office are reporting to different managers who sit outside the direct control of the central board depicted in this diagram.

The question that the board director, line manager or risk manager has to ask themselves is: "Do I have the ability to (a) tell the individuals what to do? Or do I (b) have to go through a third party to effect my instructions?" Where you have to go through a third party it is unlikely that you

Figure 1.6: Simple and complex organisations





will have any direct reporting and consequently your knowledge of the mechanisms of management of risk in the elements of the business that are outside your direct span of control is unlikely to be in any sense complete.

Again, at the risk of somewhat labouring the point, the span of control has always been an issue for organisations: look at the complex management hierarchies (command structures) effected by the Roman Army. By presenting two extremes we are only facilitating a discussion of where any one organisation sits on the spectrum from simple to complex.

Operating in the extended enterprise

The next section of this chapter explores how boards and risk professionals can begin to get a handle on this and Figure 1.7 illustrates the attributes, the features and the shapers or levers available to managers.

It is our view that there are three features of an extended enterprise to which participants will need to pay particularly close attention. These are:

Information: to what extent are you able to identify information from other participants that is relevant to the way in which you manage risk both for your own benefit, but also for the whole joint endeavour? There is little doubt that you will know the impact of failing to manage certain risks on your own objectives, but the chances are that the effectiveness and efficiency of the risk responses will be handled by other participants in the network, and unless you know what those responses are and have confirmation that they are deployed, you cannot know the likelihood of the response operating to your benefit.

For example, if you have outsourced the manufacture of components to a third party, and those components are safety-critical, how do you KNOW that the quality control is up to your standards? We know that there have been examples where banks have outsourced critical IT functions that have not been operated to the standards necessary to keep internet access to customers running on a 24/7 basis. The banks in question have simply failed to ensure that the outsource providers are running the systems to the standards required.

Governance: there is little doubt that different parts of the extended enterprise will have different approaches to the governance of risk within their respective organisations. At the end of the day, the effective management of risk

throughout the extended enterprise network will only be as good as the governance over risk and risk data in the weakest component of the network. Understanding the approach, attitudes, skills and risk data in each component becomes an important part of the context in which you can operate your own risk management processes.

Regulation: wherever extended enterprises cross either traditional industry sectors, or where they cross borders, then different regulatory environments can make the management of risk much more complicated. This has been seen in the way that the US legal authorities aggressively pursue infringements of their legal system even where the infringement can only at best be described as tangential to their territorial reach. Understanding the nature and scope of how regulators might influence the various participants in the network to behave and how that might reflect on your part of the network, or even on your own personal freedom, is an important part of the features of managing an extended enterprise.

In addition to these three features, we have identified three key shapers of behaviour amongst participants in an extended enterprise:

Incentives: to understand the likelihood of risk being managed effectively in the extended enterprise, it is critical that all participants have a clear view of the incentives that each member of the network is taking from the joint endeavour. It is widely argued that "what gets measured gets done" and this is then reinforced by remuneration policies. Of course, when we are dealing with people, it is never quite so simple: John Adams has illustrated this vividly in his book and various articles[2]. As he writes, there is a wide variety of incentives for taking risk (e.g. money, prestige, fame, love, sex) and an equally wide variety of disincentives. The issue for the extended enterprise with this first "shaper" of behaviour is to understand what exactly is going to incentivise and disincentivise both real and corporate beings that operate within this virtual meta-organisation

Ethics: the second shaper of behaviour is the nature of the ethical underpinnings that each participant adheres to in making their decisions and which guides their actions. Some would argue that we currently live in an economic environment largely devoid of positive ethical guidance, what has been described elsewhere as a post-ethical society. Nevertheless, different individuals and groups and indeed societies as a whole will take differing positions on right and wrong, on the acceptable and the unacceptable. Understanding and shaping the behaviours in divergent ethical backgrounds is endlessly difficult and therefore represents a key shaper that those charged with the governance of the extended enterprise will need to understand.

Assurance: The third shaper of behaviour is what we are broadly describing as "assurance". By this we mean: the mechanisms by which anyone in the extended enterprise knows that what they are told is happening (or should be happening) is indeed happening on the ground, often in remote locations outside of the direct reach of management control. Agreed mechanisms of control are an important pre-requisite for effective co-ordination and (where needed) risk mitigation. Clearly internal audit departments belonging to participants in the extended enterprise have a role to play, but given that (despite their mantra that they are independent) they "belong" to various participants in the extended enterprise, they cannot form the totality of the answer.

Consider a PFI/PPP scheme to build a new school, or hospital. Imagine the participants: in one corner you have an infrastructure need as represented by a local authority or by the NHS. In a second corner you have the developer who would like to construct and possibly run the facility for a considerable number of years. In the next corner there is a capital provider and possibly financial advisors (they may occupy different corners, but let's not over-complicate the example here). In the fourth corner we may well have politicians looking towards their next election. Another corner is occupied by a variety of regulators. And then there are pupils or patients, parents and relatives, teachers or hospital staff. By any account this is a complicated extended enterprise with all of the characteristics set out earlier, apart from the fact that this is probably (although not necessarily) only in one country. Ask yourself:

- Who is incentivised to do what for this joint endeavour? And who is disincentivised?
- Do all the participants share an ethical outlook? Or might some be more interested in influencing outcomes to suit their own ends rather than those of the community as a whole?
- And just how does anyone (irrespective of contractual rights) KNOW what is happening in any other part of the extended enterprise?

2. For example risk. John Adams, UCL Press, London, 1995

Preliminary steps

We think that there are several things that boards should be contemplating as they begin to explore complexity in their extended enterprises:

- A good place to start is to map the extended enterprise itself. Do you know exactly who belongs where within the ecology that is your extended enterprise? What role do they fulfil and how do they expose you to unintended consequences. One of the difficulties in doing this exercise is that while it is comparatively easy to contemplate risks similar to one that have happened in your own or others' organisations, it is much harder to contemplate risks that have never materialised. A rich combination of data showing trends and imagination to identify possible discontinuities is essential to this exercise.

- Once the extended enterprise is mapped, start to look at the social dynamics: who holds the power? It is not necessarily the biggest player: it might be the organisation that controls the supply of essential but comparatively small materials such as rare earth minerals. Think about who is getting what (financially and non-financially) from the joint endeavour? Not all rewards are directly financial. Some parts of the joint endeavour may be seeking strategic advantage for other reasons, or glory, or may be currying political favour in their home territory. Understanding their "drivers" will make a substantial difference to the behaviours that they can be expected to display when unexpected problems occur. Where are the regulatory constraints on other parties of which you might not be so familiar? And above all, what is the extent of any shared ethical values, or the absence of any such sharing that could result in the single most important determinant of success or failure.

- With those exercises in hand, it ought to be possible to start mapping some of the risks. Chapter 2 sets out an approach to looking at this problem.

However, we think that there are four things that boards need seriously to consider:

1) What is the risk appetite and tolerance for all participants in the extended enterprise? IRM wrote in 2011 about risk appetite and tolerance, but like most guidance that was written in the context of the enterprise. We think that exactly the same approach needs to be taken in looking at more complex systems of companies such as extended enterprises. We do not propose to review that guidance here but it can be accessed via the IRM website[3]. The bottom line though is that unless you understand your own risk appetite and tolerance AND that of your partners in an extended enterprise, you will not be able to manage risk with any great likelihood of success. Several facets of the risk appetite guidance stand out:

   a) What is the risk capability (in terms of capacity and maturity) of each part of the joint exercise? In other words how much risk can your partners withstand before they collapse and to what extent will you need to be ready to stand in their place?

   b) What risk data is available to everyone? Both about the elements of risk under their own control and outside their control? Much risk management is done in a data-vacuum: this simply will not be good enough. More risk data will need to be shared, including risk and control metrics.

   c) Is the balance between the propensity to take risk and the propensity to exercise control consistent across disparate parts of the extended enterprise? The chances of it being aligned by chance are extremely remote. There is little doubt that larger and older organisations tend to have a greater need for control than younger smaller organisations.

2) I also wrote in 2012 about risk culture. It might be relatively difficult to influence your own risk culture, so how much more difficult will it be to influence and change the culture of participating organisations over which you exercise little or at best transient control? Again, we point you to the guidance on the IRM website[4] so that you can share an analysis across the extended enterprise. However, we would urge you to consider:

   a) The propensity of individuals in each part of the organisation to take risk.

   b) The ethical guidelines within which people are operating: are they similar to yours, or very divergent?

   c) The extent to which incentivisation programmes influence behaviour in other parts of the extended enterprise.

3) Governance of the extended enterprise is likely to be much more complicated than governance of each

3. www.theirm.org/knowledge-and-resources/thought-leadership/risk-appetite-and-tolerance/
4. www.theirm.org/knowledge-and-resources/thought-leadership/risk-culture/

separate component. We recommend that you explore mechanisms that facilitate conversations and dialogue about risk and which embrace uncertainty and complexity. Command and control structures designed for the joint stock company of the nineteenth century are not likely to work in the dynamics of a 21st Century complex and virtual organisation. We have included a chapter on Leadership and Governance (Chapter 3) in this document.

4) Once of the most difficult aspects of the extended enterprise is that of assurance: how do boards and senior managers at component organisations assure themselves that what they think is happening is actually happening on the ground? Internal Audit has moved from compliance to being strategic partners in the pursuit of assurance. But they are necessarily compromised by the very fact that they are employed by one of the participants. We have explored the needs and potential for new models of assurance in Chapter 11.

Conclusion

We are proposing that what we need in managing this (or any other) extended enterprise is a new set of ways to look at an increasingly complex world:

1) We urgently need to rethink our models of governance. Traditional models of Corporate Governance rest on the idea of a command and control environment where the board can tell management what to do, and management can execute those instructions. Of course there is a myriad of variations on this where power may rest more with the management than the board, but the essence is the same: it is based on the concept of power residing centrally. Instead, we need to be thinking much more widely about mechanisms that can negotiate and resolve complex uncertainties in a fragile model of interdependent relationships. Into this category, I would include rethinking models of risk appetite, risk assurance, risk culture and ethics: many of the levers for managing risk which need to begin to work in this new world.

2) We need to rethink the canon of risk thinking. Enterprise risk management (or as many would call it: risk management) is quite simply not up to the job. We need to develop and popularise a variety of new tools, techniques and visualisation methods. These will need to be able to cope with the traditional mantra of risk management: identify, assess, respond, manage etc., but they need to drop the economic nonsense of the assumption that this should be done within the bounds of a single enterprise: it really does need to be done in the context of a much more complex interdependent world.

3) We need to rethink tradition models of management that we adopt in traditional bi-polar relationships: supply chain management; industrial relations. Instead we need to think of them in the context of multi-polar relations where we manage systemically (not systematically, but systemically) right across the whole of the system rather than just in parts.

Questions for the board

Throughout this document we have highlighted questions that we think the board should be addressing as they work through the issues that arise in managing complexity in 21st Century organisations. The first seven questions are as follows:

1) Has the board given adequate consideration to the risks of managing across its various extended enterprises?

2) Does the board have an approach to understanding the social dynamics (power, rewards, regulation and shared ethical values) across extended enterprises?

3) Has the board given consideration to the risk appetite and tolerance of members of the extended enterprise?

4) Has the board given consideration to the risk culture of other participants?

5) How does the board satisfy itself that it knows what is going on throughout the extended enterprise?

6) Are appropriate governance structures in place to ensure that the likelihood of success in the joint endeavour is maximised?

7) Has the board devoted sufficient resources to creating and maintaining an adequate risk management and assurance framework that function across its range of extended enterprises?

Chapter 2: Modelling the extended enterprise

Neil Allan, Elliot Varnell, Louise Gravina, Jake Storey, Christos Ellinas

The extended enterprise (EE) has often been developed in order to make more efficient use of resources (i.e. cut costs) or to extend the capabilities of the core enterprise beyond just direct suppliers and customers. However, as we will also read, the EE will often result in increased risk exposure for the core enterprise.

This can be partially explained by the nature of the increasingly interdependent world we occupy, along with the heightened number and diversity of stakeholders involved in the vast majority of modern enterprises. As a result, emergent issues and cascading failures, defined by far-reaching impact within the EE are increasingly becoming the rule rather than the exception, challenging our capacity to effectively and efficiently manage the 21st century organisation (Cantle et. al. 2013).

Functional interactions and relationships (or, connections) between stakeholders can be physical or social. In this report you will read a great deal about the social relationships – and read about some of the physical relationships too. Sometimes these relationships are overt (e.g. through the supply of manufacturing components), but sometimes they are opaque (e.g. through networks of social relationships).

Either way, they are essential to the operation of the EE which is enabled and driven by them. Technically, the EE can be described as a set of separate systems that have been coupled at various interfaces to produce intra (i.e. within a system) and inter (i.e. between self-contained systems) dependencies which can provide increased functionality – indeed create a whole greater than the sum of its parts. This, usually large, number of dependencies, along with their asymmetric distribution is a universal characteristic of complexity (see Test 1, Chapter 1) of both natural and man-made systems – the EE being an example of the latter.

When a system is complex, it can achieve increased efficiency and performance, along with increased capacity to adapt to its external environment. Alas, such systems are also increasingly sensitive to instabilities (sometimes catastrophic) and are rather fragile when central elements are affected, leading to cascades of failure. Some examples of complex systems and recent failures that have resonated within them are:

- The fragile economy that can be tipped into a recession by relatively small perturbations;
- The power grid that collapses due to a single sub-station failure;
- Relatively minor technical failures that result in huge consequent disasters in a variety of levels, ranging from economic to environmental;

Such systems are not defined by the number of components that they are composed of (i.e. complicatedness) – their degree of technical intricacy effectively becomes irrelevant. Methods for dealing with large numbers of variables are well established (ex. any form of statistical inference) and risk mitigation against failure is fairly established (ex. introducing redundancies). Rather we are facing a problem of interfaces and coupling – this is the domain of complexity where predictability and the path of causality only becomes evident post-mortem. Indeed, in a complex world, everything is obvious once it has happened (and assuming that your organisation has survived it).

Our argument in this chapter is that the EE can be effectively viewed through the lens of complex systems and as such, if we wish to be able to shield the EE, we will need to reach for modelling tools found within this domain. Complex network analysis will form the backbone of our approach, mainly due to its increased flexibility, and suitability in its inherent ethos – namely, focusing on the importance of interconnectivity rather than the discrete elements themselves. The interested reader is referred to the extended technical reviews of Albert and Barabási (2002) and Newman (2009). Other tools that are found within the domain of Complex Systems do exist - examples include: System Dynamics, Bayesian networks and Agent Based Modelling.

5. Complex network analysis is a scientific field which is currently attracting a lot of attention as it can provide an analytical toolkit for the analysis of real-world systems. It has emerged by empirical observations across systems of different domains but of which similar patterns appear to unite them – systems ranging from the human brain, the economy, shipping routes and inter-organisational communications.

A network toolset for extended enterprise risk

As a part of a network systems approach, it is necessary to decide where the boundary of the EE lies and what is worth including. The key here is to be explicit about which stakeholders are considered to be inside the EE, which are outside but need to be included in the analysis, and those which are outside the EE and are not going to be included in the analysis. Reasons for non-inclusion might be stakeholders that cannot be controlled, difficulty in obtaining meaningful data, importance or simply expediency. Remember that a model needs to be as simple as possible but not simpler.

Once all the relevant stakeholders are identified, we have the set of nodes that will form the basis of our model. The next step is to think about how they are connected – such will result in a network which is an effective abstraction (and thus, a model) which can allow further analysis and insight on the potential risks of that the EE may be exposed to. The following example is intended to illustrate the basic steps and parameters involved in mapping such network (a systematic process is also included in the form of a flow chart – see Figure 2.7), followed by typical insights that one may infer from such an approach. In a way, it paves a methodology on how suitable paradigms can be used to map a real problem into an abstract model, along with typical insight that can be gained by applying a set of analytical tools on such model.

We should note that the proposed methodology is purposefully described at a high-level in order to ensure generalizability and applicability to a range of practitioners, irrespective of the specifics of their own challenge. Nevertheless, it is strongly recommended that a more detailed analysis on a case-by-case scenario is further produced, building on the suggested approach, in order to maximise the relevance and utility of the insights.

Example

Yam Yam Ltd. is a fictional enterprise which competes in the consumer retail market and its main income revolves around 3 core products – A, B and C. Typical of such an enterprise, it has a number of internal departments the Buying, Product Managers, Finance and Quality Assurance. A major competitor in the market also exists, producing product 1. Figure 2.1 illustrates a typical internal communication network– an information exchange process which enables the organisation to perform its function.

Outside this organisational core, one expects to find an underlying supply chain. Its fundamental purpose is to increase the value of raw material by converting it to a final product. Thus, its efficiency and robustness is critical for the profitability of the EE. One might expect to encounter increased complexity within such systems as the EE attempts to increase the value obtained by this process along with conforming to changes in its operational environment (ex. new legislation introduced etc.) – usually in terms of increasing flexibility, adaptability, efficiency, robustness in order to attain a competitive advantage. Typically, such supply chains will be composed of a number of stakeholders at a variety of tiers and the nature of connections between them can be money flow, contractual obligations or material flow. In this example, we will focus only the material flow aspects, simply for the sake of clarity and generalizability. The output of the process provided by the supply chain will then follow the distribution channels in order to reach the final customer. The intermediate stops between the outputs of the supply chain and the customer will vary depending on the context of the EE – typical composition of the distribution channels in retail will include depots, distribution centres and retail units. The rather simple supply chain and its underlying distribution system which mobilises Yam Yam Ltd. can be seen in Figure 2.2.

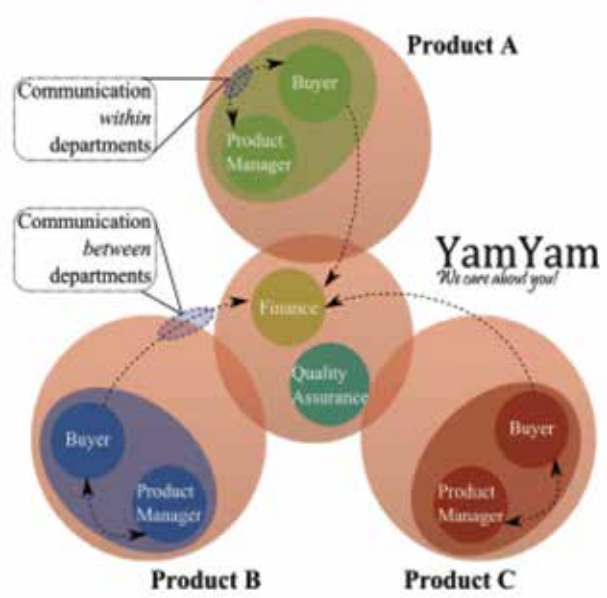


Figure 2.1: Simple retail enterprise system. Of interest are both presence and absence of communication links. For example, notice the presence of direct information flow links within Product Departments but also between the latter and the Finance Department. Interestingly, notice the lack of direct communication between Product Mangers and the Finance department – potential implication can include delayed decisions taken by the latter etc.

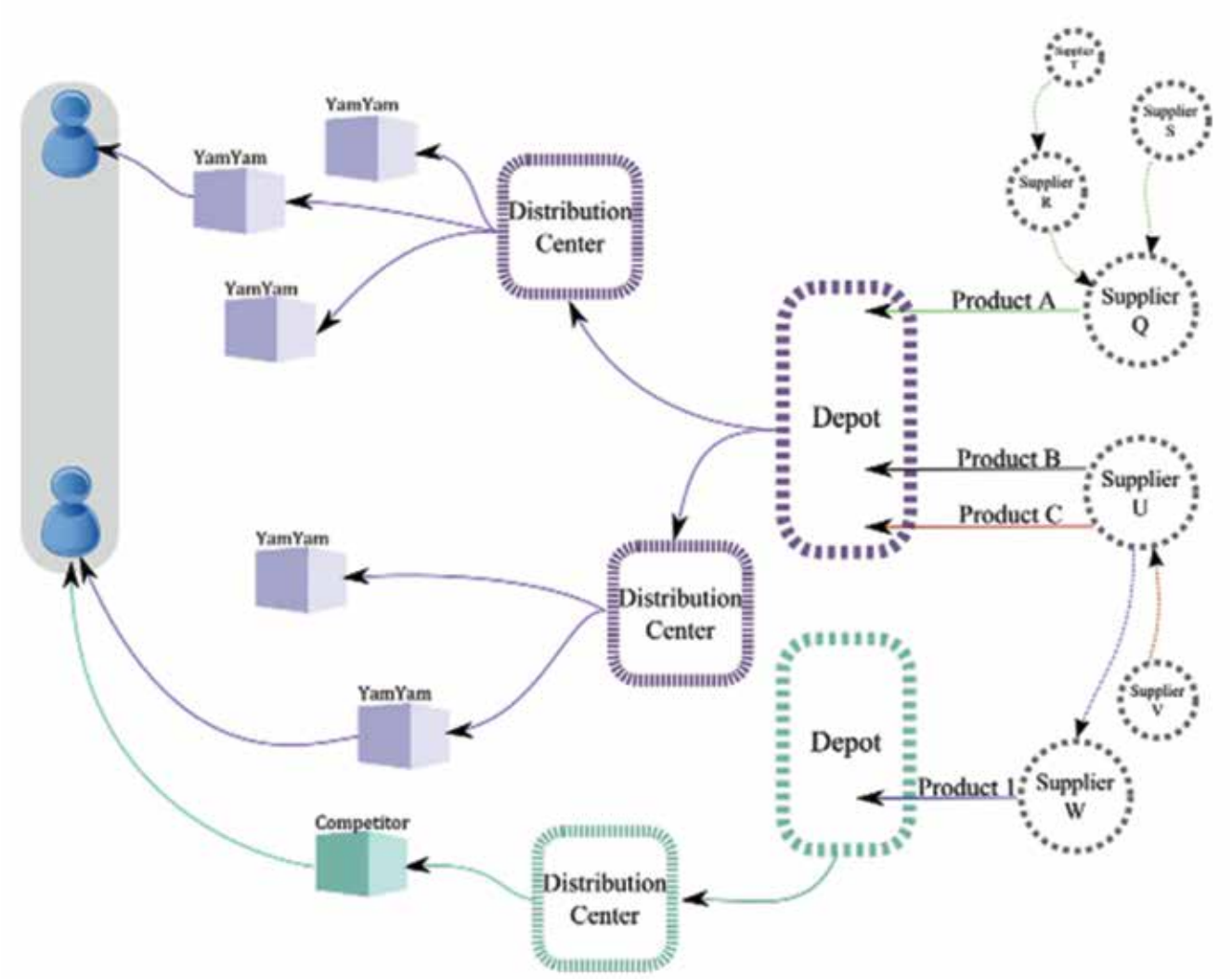


Figure 2.2: Typical distribution/supply chain system for Yam Yam Ltd. Within this context, the size of each node represents the output of each stakeholder in terms of value, the dotted lines represent a transient material (i.e. cannot be directly marketed to a customer, though can be exchanged at a suppliers level) while a solid line represents the flow of a marketed (i.e. final) product

We can now inflict a more realistic notion on the operational aspect of the supply chain – effectively ask the question of what enables the supply chain to operate. One vital element is its interaction with the transportation system, as it is coupled to the interactions of the stakeholders within the supply chain i.e. the system that enables the suppliers to interact with each other – see Figure 2.3. Risk materialisation that can affect the transport system will inevitably resonate through the supply chain, as suppliers will not be able to interact as planned, hindering the function of the EE as a whole.

Using Figure 2.3, consider Supplier T (with a relatively small output) who is only able to transport its raw material to Supplier R by shipping. The port of which exportation takes place is highly dependent on the ability of the material to be transported there i.e. from the farm to the port, through the rail system. Thus, the ability of the supply chain to function (i.e. for stakeholder R to interact with T) is entirely dependent on the ability of the transportation system to function as expected. Notice how the inevitable dependence of the supply chain to the transportation system of a (potentially) foreign county has substantially altered the risk exposure of the EE. Political volatility in terms of future expansion of the transportation system, new legislation controlling its capacity, weather conditions of which the transportation system is exposed to, the degree and diligence that maintenance works is applied etc. have now been added to the list of risks which can significantly impact the ability of the EE to function.

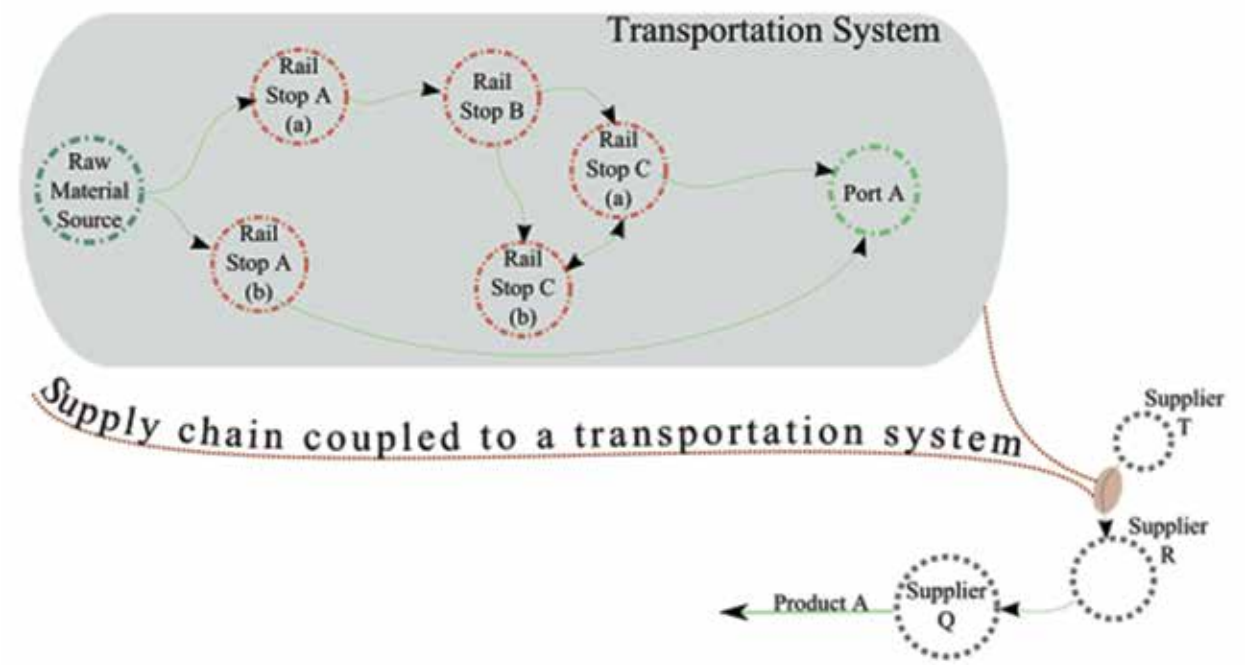


Figure 2.3: Connection of the supply chain and the transportation system. The operation of the former is conditional to the operation of the latter, however the risk exposure of the former is entirely different than that of the latter. Such coupling can induce cascading failures which resonate within the EE on a much grander scale as one may initially anticipate.

The materialisation of any such risks can, for example, hinder the ability of a supply chain stakeholder to utilise the usual route to export, upon which characteristic delivery times are calculated – for example consider the inability to use the Rail Stop A(a) due to signal failure – see Figure 2.3. Consequently, another route must now be chosen, which will inevitable cause delays and increased costs for both the stakeholders involved and, as a whole, the EE. As such, the capacity of the enterprise to undertake its function, as expressed through both business promises (i.e. contracts) and implied security (ex. insurance) has effectively been compromised simply because of interdependencies found between two coupled systems that have entirely different operational regimes (and inevitably, exert different risk management practices). The resilience of the EE is evidently as strong as its weakest (or more suitably, *exposed*) component.

It is now becoming evident that even the trivial example of Yam Yam Ltd. is evolving into a rather complex EE. Again, it is worth noting that this evident complexity has not been a product of increased number of components (i.e. scale) but rather an issue of interfaces. Arguably, being able to understand the shifts in terms of risk exposure as various interfaces are uncovered is of great importance for the understanding the real EE. Uncovering the key constituents of a complex situation is the first step in order to construct a much simpler model which we can fully understand and thus, model and predict certain aspects of the EE. In summary, let us first identify some key elements that have shaped its complexity profile by piecing the picture together – see Figure 2.4.

From right to left:

Yellow Boundary: represents the core enterprise and some of its composing elements (for this specific example, viewed from an organisational point of view) and how the functionality of the core emerges by the interactions (in this case, mainly revolving around information exchange) between self-contained entities in the form of departments.

Purple Boundary: The number of relevant stakeholders (and their respective interactions) is expanded by adopting a material flow view. Specifically, we now focus on suppliers and physical structures. From this perspective, the functionality of the core enterprise expands from mere management to the provision of tangible products, enabled by the interactions (in this case, material flow) of the aforementioned physical components.

Grey Boundary: A further aspect which serves as a vital infrastructure of the interconnections within this layer to take place is also introduced – in this case we have used the example of a transportation system that enables the material flow to take place (in the case of the Yellow boundary, such enabling infrastructure could include

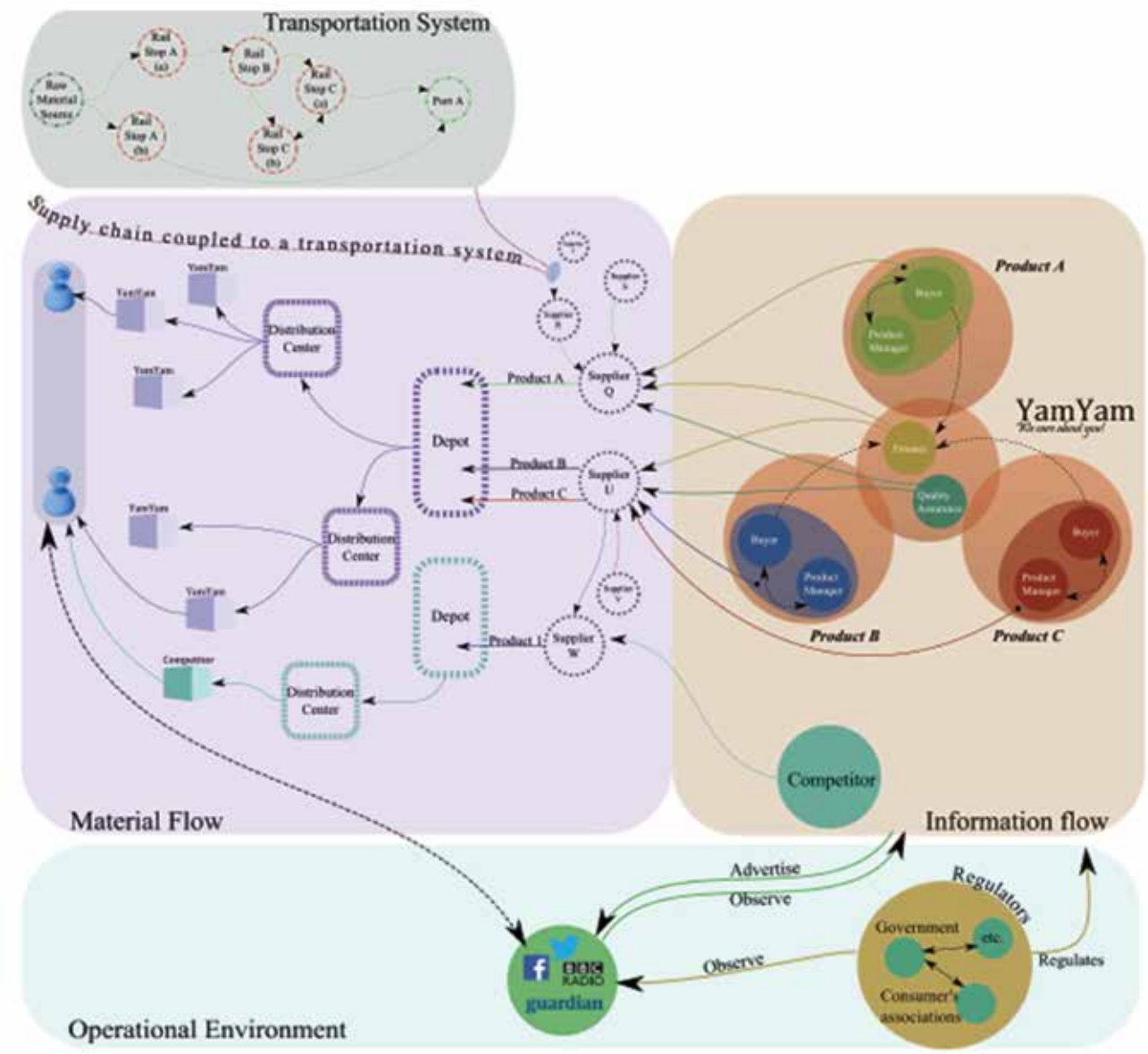


Figure 2.4: The Extended Enterprise Network of Yam Yam Ltd, within the context of four distinct, yet interdependent, elements.

computer networks that enable individual between and within the departments to communicate and exchange relevant information etc.). The transportation system, and its subsequent coupling to the material flow, is again another aspect which can influence the functionality of the entire enterprise – failure in the function of the former will inevitably affect the capacity of the latter to perform one of its key business aspects; namely deliver physical goods per agreed conditions.

Cyan Boundary: Lastly, the cyan layer introduces the peculiarities found within the operation environment of the EE – in this case two such systems include media and regulatory agents. To further elaborate, consider a wave of customers expressing their dissatisfaction on the condition of a product though social media. Such action is expected to be noticed by relevant regulatory boards and potentially initiate reforms that can substantially impact the capacity of the EE to operate profitably. Notice that at no point the EE has any direct influence (or control) on the aforementioned causal path.

The extended enterprise

The entirety of the systems included in Figure 2.4 share a fundamental aspect; they all have the power to meaningfully influence the capacity of the EE to function – thus, they play a significant role in the *control* structure

that drives such enterprise. This observation will form the cornerstone of our approach towards defining, describing and understanding the EE network and its subsequent risk exposure. The following section will attempt to abstract the specifics of the introduced example in order to construct a generalizable methodology.

A generalised model for mapping the extended enterprise

Our aim in composing this chapter is to provide something that can help practitioners with their decision making under their unique situation, in terms of the aforementioned EE network. In order to do so, it is necessary to first describe the EE in terms of its behaviour, form, viability and purpose.

Additionally, it is important to identify the environment within which the EE is operating, as the latter can be shaped by domain-specific forces and exposures –the operational environment. Furthermore, in order to consider what enables the EE to perform its function, one needs to closely examine its resource environment. Figure 2.5 illustrates the relationships between these concepts on an abstract level in order to help their identification.

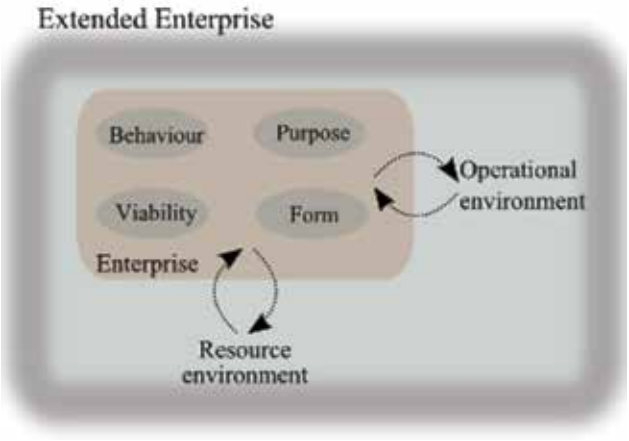


Figure 2.5: Generic Enterprise Model – adapted from (Hitchins, 2008)

In relation to Yam Yam Ltd. the resource environment is effectively the supply chain (Figure 2.4, Purple Boundary); enabled by the transportation system while the operational environment is where the regulatory agents and media influence (Figure 2.4, Cyan Boundary) come into play. Finally, Yam Yam Ltd. can be defined by understanding its form (i.e. internal organisation structure – Figure 2.4, Yellow Boundary), its viability (e.g. capacity to reduce its exposure by leveraging other agents such as suppliers, insurance etc.), its purpose (e.g. long-term growth) and its behaviour (e.g. ethics and culture).

Identifying stakeholders

As soon as the boundary of the EE is determined, key entities (i.e. stakeholders) that can influence its function need to be mapped. In order to do so, an appropriate property needs to be selected in order to filter out irrelevant stakeholders or agents. In this case we are interested in the ability to exert some sort of control on the components of the EE – see Figure 2.6. Note that this aspect further enables to answer Test 3, as introduced in Chapter 1.

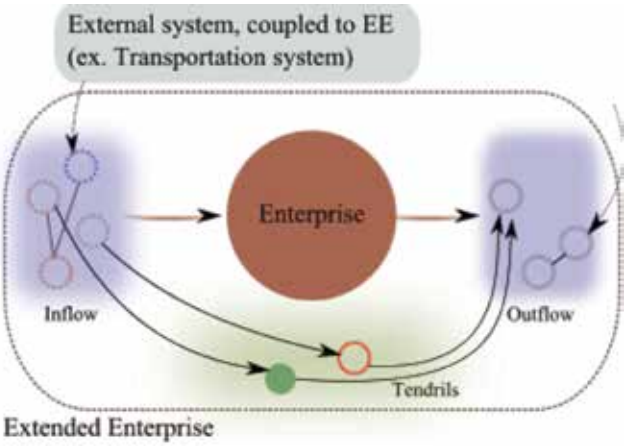


Figure 2.6: Generic Control Structure for an Enterprise. Empirical observations confirm the existence of such structures in a number of complex systems ranging from the economy to the WWW. For examples see (Dorogovtsev and Mendes, 2002, Vitali et al., 2011)

Stakeholders found within the inflow directly exert (meaningful) influence on the enterprise but cannot be influenced by the latter (in terms of the Yam Yam Ltd example, Figure 4, Grey Boundary contains agents of this sort). Similarly, agents found in the outflow are those who are being directly influenced by the enterprise but cannot directly reciprocate. Importantly, some stakeholders do not interact with the enterprise itself but can have a substantial, indirect, influence upon it, as they can influence the reciprocity capacity of the agents found in the outflow without the ability of the enterprise to effectively act against it – such stakeholders are found within the tendrils of the system. With reference to the Yam Yam Ltd. example, such agents can be found in Figure 2.4, Cyan Boundary. Finally, notice that this approach can further accommodate for the influence of external factors such as externally coupled systems.

Defining the interactions

The next step is to shift the focus from the single, discrete stakeholders to the nature of their interactions.

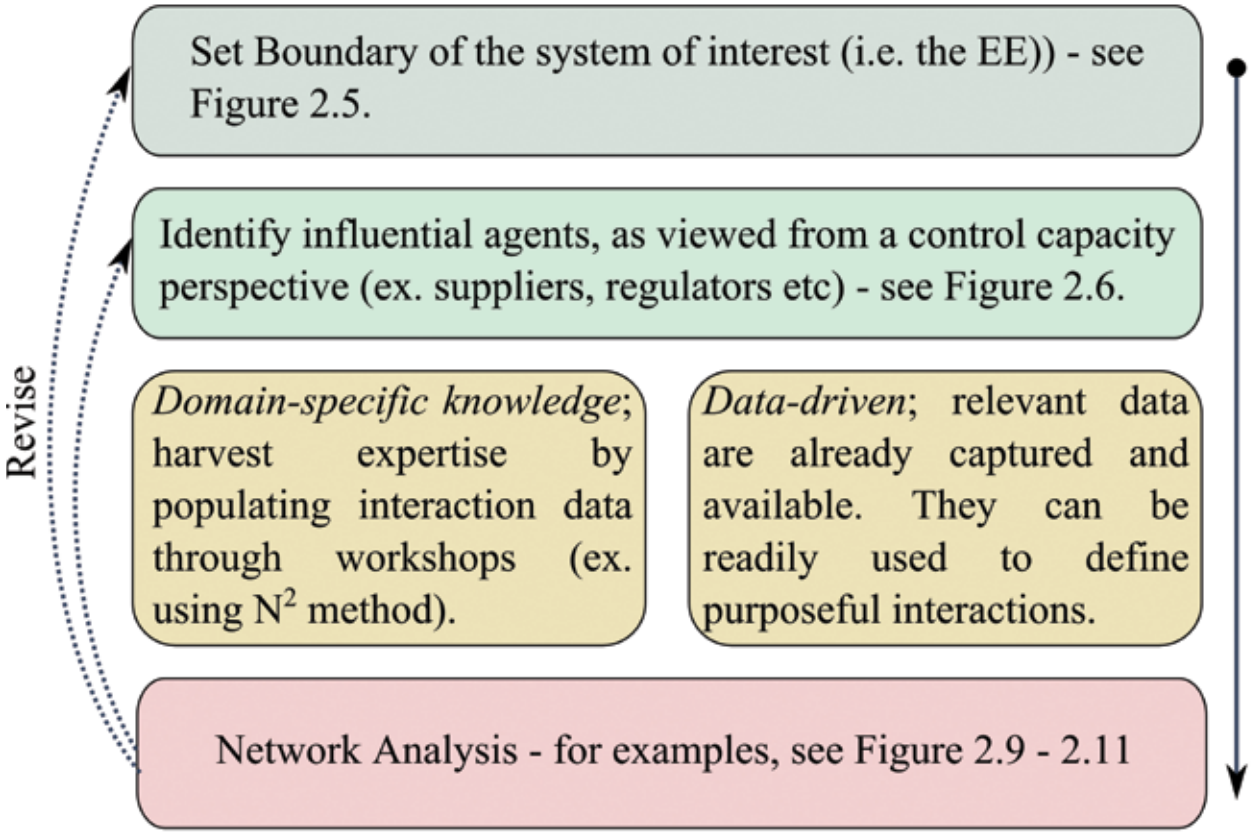


Figure 2.7: Process flow for creating an Extended Enterprise network.

This might include factors such as information exchange, material flow, regulatory agreements, money flows, social interactions and even organisational hierarchy. Alternatively it might be just domain expertise that determines the connections – see Figure 2.7 for a complete process that can aid in transcribing a real situation to an analytical network model.

Once information about the nature of the interactions is collected a network is created upon which we can perform analysis and simulations. This network can then enable detailed scenario testing, for example, to stress-test the enterprise on both internal but also external shocks that may materialise due to its exposure in fast-evolving, dynamic environments and complex connections. Such models can further provide useful insights on how local failures (e.g. a number of elements under-perform or become non-functioning) can influence the performance of the entire EE. Consequently, key stakeholder (or in more general terms, *nodes*) in the network can be identified to ensure that these have extra levels of security or risk mitigation measures in order to ensure the likelihood of local tipping points controlling the operation of the EE is minimised.

Before being able to explore these questions, the required level of aggregation for doing the analysis needs to be decided. This aspect can be ideally driven by the question, but in reality, other elements such as the nature of the data itself and the need for expedience can influence this decision.

Complex networks analysis

Complex networks is a scientific field which is currently attracting a lot of attention as it can provide an analytical toolkit for the exploration and modelling of real-world, complex systems –see Barabási (2007) for a brief overview. Generally speaking, it is possible to analyse any such network at two distinct levels of detail – at a local or global level.

Local level

A significant part of complex networks analysis revolves around the identification of central nodes (and thus, can be considered to be of a local level) in an attempt to identify drivers that can dictate the dynamics of

the entire network. A variety of different approaches exists within the field, though they can be roughly categorised thematically in terms of the individual node; the distance between the nodes (closeness); the ability of a node to control some sort of flow within the network (betweenness) and the importance of a nodes' neighbours. They can be briefly described as follows:

Degree centrality – how well connected a node is i.e. number of in/out coming connections. Such nodes will most likely be the most visible node in the network as they will be connected (and thus visible) to a greater number of nodes. Such examples may include highly connected individuals in a social network, well-connected manufacturers within a sparse industry, major financial institutions within the economy etc.

Closeness centrality – how easily a node can reach any other node i.e. how close it is to its neighbours in terms of hops. A node is central in terms of its distance to other nodes; a node with great distance can be interpreted to have greater autonomy. A typical example is the emergence of important cargo airports acting as distribution points with minimum distance between export and import points (such as Hong Kong International Airport, sitting between China, a major export source, and Europe, a major import point) – this is partly due to their high closeness centrality within the considered network (i.e. available airports)

Betweenness centrality – how important a node is in terms of connecting other nodes. This measure can be interpreted as a measure of control upon something that flows through a network. High node betweenness can often result in bottle-necks which can be of great importance in keeping a network flowing. Reflecting back on Figure 2.2, the Depot can be intuitively identified as a bottleneck (and thus, possesses high betweenness) as if one were to remove it, the network would immediately become disconnected and material flow from tier 1 suppliers to distribution centres would have been restricted.

Neighbour's characteristics – how important, central or influential a node's neighbours are; effectively representing the idea that "you are as important as the people you know". This idea is typically used by internet search engines and builds on the idea that a node is as important as its neighbours' are. In terms of supply chains, one may consider a stakeholder who provides a single (i.e. very low connectivity) but much bigger stakeholder with a relatively low-value material. Nevertheless, if this material does not flow from the former to the latter, the impact will be great as the big stakeholder will not be able to perform its function. Under this perspective, the relatively low output, low degree node can be considered to be of great importance.

Global level

One may also wish to characterise networks in order to allow global comparison between other networks to compare the inherent robustness of the EE. Such global measures include:

Network Distribution – the mapping of how connections are distributed amongst nodes. Such measures can indicate whether the network is homogeneous (i.e. every node has more or less the same number of connections) or heterogeneous (i.e. every node has very few connections with occasional super-connected nodes). The implications can be of great importance as the effect of local failures on the overall system are qualitatively different – see Figure 2.8.

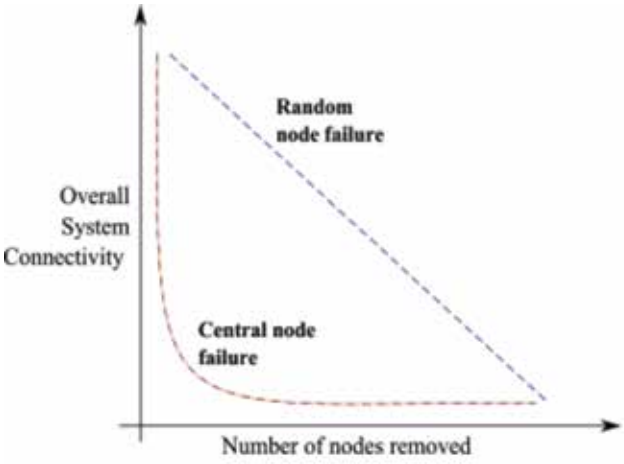


Figure 2.8: Typical behaviour of a complex system under node failure. Evidently, complex systems are relatively robust to random failures but extremely vulnerable to targeted (i.e. central node) failures. This behaviour is fundamental for such systems and is encapsulated via the term "Robust-yet-Fragile".

Network Density – the ratio between the connections found within the system and the theoretical maximum that the network can accommodate for. A network in which all nodes are connected with all other nodes will have a density of one. Highly connected networks may imply that individual connections are not so important, but may also imply, that such EE is highly sensitive to any kind of perturbation.

Network complexity is related to network density and network distribution in two ways, based on the assumption that increasingly convoluted network structures demand higher operational resources.

- Network density is conceptually linked with network complexity because a denser network requires more effort to build and maintain.

- Network distribution implies higher coordination costs as highly connected nodes will require much more effort to coordinate.

Modelling

Understanding and adequately mapping such network characteristics can contribute to understanding a number of peculiar features of complex systems. For example, the "Robust-Yet-Fragile" nature observed in a number of systems such as the Internet, the power grid etc. can be attributed to their underlying degree distribution (Doyle et al., 2005). Under specific configurations, random failures have little impact while failure of "central" nodes can have disproportionate effects on the overall performance of the system, assuming of course that the latter is dependent on its inherent connectivity ex. a transport network is enabled by its mere ability to connect nodes with

links. Supply chains are typically described by similarly heterogeneous distributions, and thus, can be expected to behave in a similar fashion.

However, a note of caution should be made here as the majority of suitable methods that can be used (including System Dynamics, Bayesian Networks and Agent Based Modelling) are sensitive to the initial parameters and thus, carefully tailored models should be constructed. A number of exogenous factors should also be considered and introduced within any such model – such factors may include inflation and interest rates, product demand, labour, resource and energy costs etc.

Using the process entailed in Figure 2.7, we have illustrated how this general methodology can be applied to the simple (in terms of scale) but surprisingly complex (in terms of interfaces) example of Yam Yam Ltd. As such, we have identified both key nodes (i.e. suppliers, organisational departments etc.) that need to be acknowledged within the model, along with their assigned interactions. Notice that only one kind of interaction will be considered (i.e. material flow) as the aim of this example is to illustrate a methodology and a set of tools rather than present an elaborate analysis with limited transferability, and thus, usability to a practitioner. The analysis will exemplify some of the key metrics mentioned in the previous sections, along with typical interpretations that may be applied. Nevertheless, the importance of a detailed analysis on a case-by-case approach in order to deliver truly applicable and relevant understanding cannot be overstated.

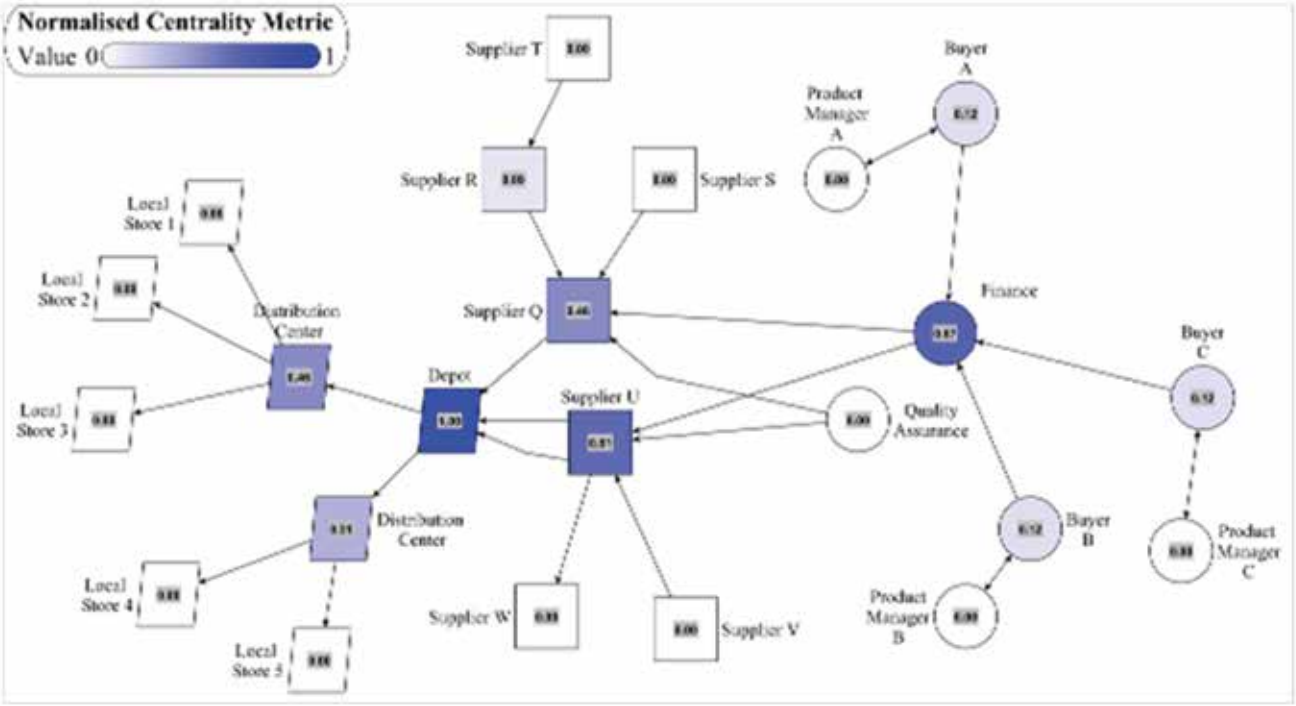


Figure 2.9: Node Betweenness Analysis results. Note that results are normalised – the darker the hue, the higher the value.

Network analysis using Yam Yam Ltd.

Node betweenness

Node betweenness allocates centrality on nodes depending on their ability to control a flow of a material throughout the network. This sort of information, used in conjunction with knowledge of the system can provide meaningful insights into the possible risks to the EE based on the network interactions. Within the context of Yam Yam Ltd., and using the quantitative results captured in Figure 2.9, the following observations and deductions can be made:

- The Finance department within the organisation, along with the Depot found within the distribution network, are clearly highly central to the EE as they control the majority of flow in terms of information within the organisation, and material within the distribution network respectively.
- Consider the control of a supplier upon the final output of a product (i.e. the Depot's output). Supplier R has a higher centrality score when compared to other second tier suppliers. Specifically, in order for Supplier Q to provide the final product, Supplier R must enable the flow of material originating from supplier T; this is not the case in term of Supplier S for example. Thus, Supplier R may not be the most connected (and thus most visible) entity within the supply chain but can potentially create a cascade of failures as it sits within a critical position of the network.
- In the case of a potential contamination within the network, the betweenness metric allows us to identify which parts of the extended enterprise are more exposed by highlighting the weak links. For example, one can identify Supplier U having an increased capacity for spreading a contaminant within the network as it is able to control a higher number of flows when compared to any other supplier – notice that this is not as obvious as one would expect since it contains exactly the same number of incoming connections. Similarly, one can signify the Depot as being the single most prominent entity as it essentially connects the two clusters by enabling all processed material to reach customers – thus highlighting their capacity to enable cascades within such a system.

Node degree

Degree analysis, as previously mentioned, refers to the number of connections a node has. Clearly this can be approached from two perspective; mapping either the in- degree (i.e. incoming connections, see Figure 2.10) and/or the out- degree (i.e. outgoing connections, see

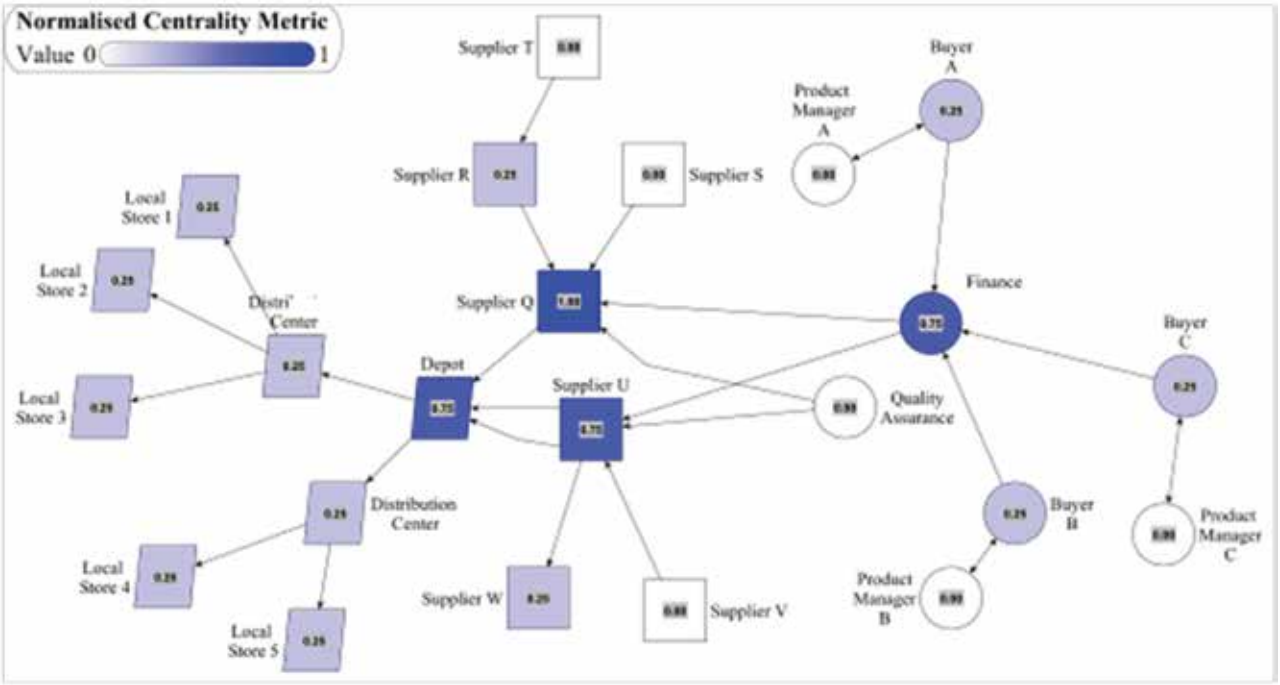


Figure 2.10: In-Degree Analysis (number of incoming connections to a node). Note that results are normalised – the darker the hue, the higher the value.

Figure 2.11). Such measures can have a number of useful interpretations, though one needs to be explicit on the nature of the connections to make operational sense and draw risk related conclusions. A number of simple but interesting interpretations about Yam Yam Ltd. can then be made from degree analysis when we use information flow as the context of the connections.

Firstly, the finance department within Yam Yam Ltd. has is defined by a high in-degree centrality. This makes sense as it probably deals with a heavy flow of information from buyer exchanges and such analysis might highlight the potential to generate risks that can incur from mishandling information. Also, it will be most sensitive to perturbations in other parts of the organisation downstream. Thus, it would imply that an increased attention should be given to managing and mitigating such lapses in information flow, particularly as it is also highly ranked in terms of between-ness (see Figure 2.9).

However, once the out-degree perspective is introduced, (Figure 2.11) both the Finance and Quality Assurance control become equally important. One might ask why finance and Quality Assurance are not more closely connected and maybe this is an area of possible risk mitigation. Remember this is only a simple simulation and in practice of course both departments may communicate with each other and also have a much broader set of inward and outward communication

It is also worth noting that in Figure 2.10; Supplier Q has a higher number of incoming connections than the other suppliers but a lower number of outward connections as shown in Figure 2.11. This is interesting as it places Supplier Q in a very important position to influence the supply to the Depot and it is also a central pin in its own mini network. This is also confirmed by its between-ness ranking in Figure 2.8. Any failure by Supplier Q would disproportionately impact distribution and supply to the stores. Common sense of course in the simple Yam Yam Ltd. example but the point being that this is backed up by analysis which can be applied to large networks. By overlying different networks and different metrics, a clear picture of key nodes and key relationships becomes apparent, this provides for an invaluable risk management tool.

The observations in this simple case study are quite trivial and somewhat obvious, but the power of this technique is to highlight risky areas in the network when they are much larger and opaque to any one person in the EE. By making explicit the connections and their interactions it is possible to reduce the complexity of the EE, and help risk managers spot higher risk elements across disciplines and stakeholder groups. It can also be used as a useful scenario testing model by taking out certain nodes or connections.

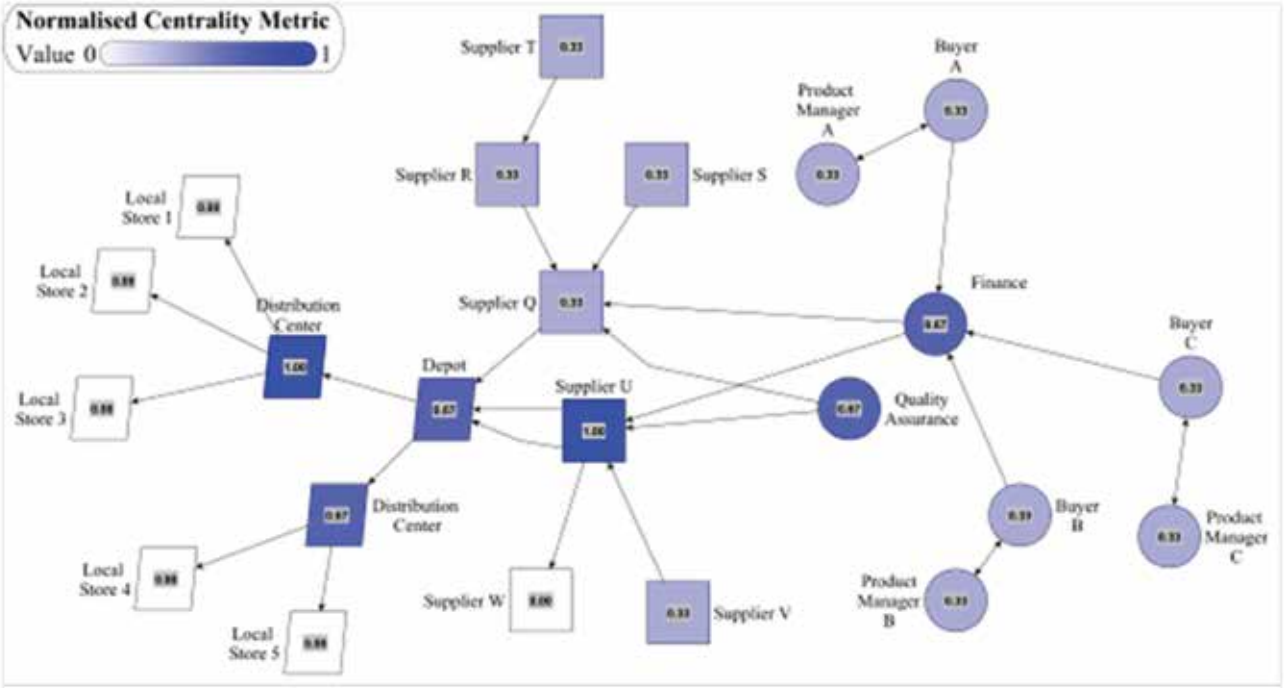


Figure 2.11: Out -Degree Analysis (number of out-going connections from a node). Note that results are normalised – the darker the hue, the higher the value.

Summary

The purpose of this chapter was to introduce a methodology to abstract the extended enterprise (EE) into a tangible model which can then be analysed and used to aid decision making, from a risk perspective.

A simple example was first introduced in the form of a fictional origination, Yam Yam Ltd., which was slowly built-up from simple obvious set of connections to a more complex EE with multiple interdependent connections. It illustrates the importance of interactions and how they can alter the risk exposure profile of an EE and subsequently how the function can be influenced. A generalised model was introduced (Figure 2.5 & 2.6), along with a mapping process (Figure 2.7); in order to illustrate how the process can be applied to any situation or EE. The analysis can provide meaningful and usable insight in to potential risks, as presented in the final section of the chapter.

Take away points

- Modern organisation are striving to achieve more with less by coupling a number of their activities to external systems; for the purpose of this chapter, this is the essence of the EE.
- Complex networks are a powerful modelling framework that has been successfully applied in a range of complex systems, from the human brain to the economy. As EEs are becoming increasingly similar to such systems (due to the inter/intra connections), this framework can serve as a great step in improving our capacity to manage, control and protect the EE.

This chapter has laid down a process flow in which a set of tools has been introduced in order to aid a practitioner in mapping the EE as a complex network. A fictional example was used in order to enable reflection between theory and application, a sense on the data that may be needed and finally, an interpretation on the analysis results.

References

ALLAN, N., CANTLE, N., YUN, Y. & GODFREY, P. 2013. A review of the use of complex systems applied to risk appetite and emerging risks in ERM practice. *British Actuarial Journal*, 18, 01.

ALBERT, R. & BARABÁSI, A.-L. 2002. Statistical mechanics of complex networks. *Reviews of modern physics*, 74, 47.

BARABÁSI, A.-L. 2007. The architecture of complexity. *Control Systems*, IEEE, 27, 33-42.

DOROGOVTSEV, S. N. & MENDES, J. F. 2002. Evolution of networks. *Advances in physics*, 51, 1079

DOYLE, J. C., ALDERSON, D. L., LI, L., LOW, S., ROUGHAN, M., SHALUNOV, S., TANAKA, R. & WILLINGER, W. 2005. The "robust yet fragile" nature of the Internet. *Proceedings of the National Academy of Sciences of the United States of America*, 102, 14497-14502.

HITCHINS, D. K. 2008. *Systems Engineering: A 21st Century Systems Methodology*, Wiley.

NEWMAN, M. E. 2009. *Networks: an introduction*, Oxford University Press.

VITALI, S., GLATTFELDER, J. B. & BATTISTON, S. 2011. The network of global corporate control. *PloS one*, 6, e25995.

Chapter 3: Leadership, management and governance in the extended enterprise

Prof David Welbourn, Prof Dean Fathers

This chapter focuses on the reality that governance has more to do with people, behaviours and relationships than it has to do with processes and structures. To understand what constitutes a sound approach to both governance and risk management across the extended enterprise, it is necessary to understand that the demands and styles of leadership and management that contributed to organisational success are no longer sufficient to guarantee success in the world of complex adaptive behaviours that are much more prevalent in this context.

Introduction

It will be clear from this collection of resources that the step of broadening thinking beyond individual organisations to the extended enterprise is more than a matter of scaling existing principles. What may be less evident is the extent to which we have to escape the boundaries of traditional thinking before we can begin to make anything more than superficial inroads into the challenge.

Our whole philosophy and understanding of organisations, their structures, the management processes, regulation, performance, risk, and accountabilities – to select just a few of the bedrocks of governance – are based on a view of the world that Meg Wheatley[1] has described as Newtonian. This classical world is one in which causality is largely linear and predictable, organisational constructs are dominated by hierarchical thinking, and although we may need complicated analysis, problems in the main have logical solutions that can be determined if only we have the patience, computing power and suitable frames of reference for measurement.

We know instinctively that such a utopian state is beyond our reach, but we cling fast to the sure belief that the foundations on which we have built both our practical experience and theoretical concepts are a sound and sufficient basis.

But in organisational sciences, we stand as it were at a period equivalent to the dawning of the 20th Century for the physical sciences, when our Newtonian world was about to be rocked in every conceivable direction, as relativity, quantum physics, field theories and chaos would usher in a world of new understanding that would begin to explain some of the unanswered questions, whilst at the same time predicting and then demonstrating undreamed of phenomena (when the laser was first predicted, there was neither known mechanism to create one, nor any inkling of what purpose they could serve, yet they are now ubiquitous in the fabric of society's infrastructure).

As we move the locus of our organisational studies towards the extended enterprise, it is as if we are at this same dawning, holding fast to the Newtonian roots and struggling with the primitive understanding of what will ultimately become the Quantum age. And continuing the analogue a little further, what we might loosely group as the quantum sciences demonstrate that in 99% of cases, Newtonian models are still relevant and sufficiently accurate to describe our world. The fresh insight from our new science though, has shown us precisely when and how traditional models fail, but we have yet to reach an equivalent realisation in organisational sciences. Like even the great Einstein, we baulk at the ineffable nature of some of the emergent thought. Over time though, the frontiers of physics have continued to blaze a trail past the superstitious declarations: "here there be dragons!", developing our understanding, and delivering both tools and knowledge that continue enhancing our lives, some of which are accessible to the lay population, and others which are the preserve of the specialist.

As Oliver Wendell Holmes[2] stated more than a century before its true significance was recognised "*I wouldn't give a fig for complexity this side of simplicity, but I would give my right arm for simplicity the other side of complexity*". Our aims to develop organisational and leadership science into this new world demand the confidence to explore the complexity, before translating the consequential impact into simple, clear and profound messages.

Establishing a new foundation

If we are to build a new understanding for this world of the extended enterprise, then we need to build a new framework around principles that prepare us for the emergent "quantum-like" organisational science. In this section, we expose some of the shibboleths of our "Newtonian" world to the need for fresh understanding.

Whilst the number of definitions abound, traditional models will be characterised by the following broad definitions:

- **governance** refers to the set of structures, processes and relationships within which decisions are made, resources deployed and accountability is managed, to achieve agreed goals;
- **management** is the process of allocating and controlling resources towards an agreed set of goals and outcomes;
- **leadership** is the process of influencing (inspiring) followers to work towards a shared vision;
- **regulation** involves two distinct purposes – enforcing compliance with defined standards, and, in cases where there is an asymmetric power relationship, acting on the side of the weaker parties to prevent abuse by the more dominant party;
- an **organisation** is a bounded autonomous entity with defined governance and accountability structures over which the governing body has controlling authority and relative freedom to determine purpose, action and behaviours;
- **risk** and **uncertainty** reflect different ways in which uncontrolled factors impinge on the achievement of goals and effective management is a vital aspect of governance: generally the term risk applies to quantifiable probabilities and uncertainty refers to the unknown and unknowable.

In preparation for our new framework, additional definitions are required:

- a **system** or **extended enterprise** is a complex interdependent and interconnected set of entities where the actions and behaviours of one entity interact with those of its neighbours within the system;
- markets, networks, collaborations/ partnerships and movements are all different types of system, characterised by different forces and power relationships between the component entities in the system;
- a **complex adaptive system** is one in which the numerous relationships within the system are not static (or passive) but are determined by an active or adaptive process, which gives the system the potential to learn and adapt its behaviour based on both context and previous experience.

The new paradigm will be built at system level, frequently one that is complex and adaptive.

It is important to understand some of the interesting properties of complex adaptive systems, which make the analogy of quantum science particularly apposite[3]:

- even if it were possible to know everything there is to know about the system, it would be impossible to predict precisely what will happen to that system, but it is possible to discern the probable range of outcomes;
- the process of observing and measuring a complex adaptive system, changes its behaviour (in the same way that simply asking someone's opinion on a subject primes their thinking, thus influencing how they respond);
- the boundary between simple and complex adaptive systems is not static – when simple systems are placed under sufficient stress, they begin to exhibit behaviours of complexity;
- complex systems are often characterised by turbulent conditions described as VUCA – comprising Volatility, Uncertainty, Complexity and Ambiguity[4-6];
- the combination of VUCA forces often creates chaos and disorder (as defined by the science of chaos theory) increasingly manifesting as paradox, in which apparently conflicting and contradictory factors are observed – so much so, that Gleick[7] in his prologue, echoes Wheatley's observation about the boundaries of classical thought "where chaos begins, classical science stops".

Laurence J Peter[8] understood the difficulties posed by this new world, when he said: "*Some problems are so complex that you have to be highly intelligent and well informed just to be undecided about them*."

The implications of the new paradigm

The most immediate observation arising from the combination of ingredients in this new paradigm is that whilst performance improvement in organisations or simple systems can be brought about by stronger control, this is not true in complex systems. A complex system cannot be controlled, since its final state can never be predicted accurately. It can, however, be influenced. The more the system has a propensity for adaptation and learning, the greater the probability that it can be influenced or nudged into the desired state.

The profound revelation from this understanding is that traditional management (control of resources) becomes ineffective in complex systems, but strong leadership (that seeks to use influence to guide people towards the shared vision) can achieve the desired results.

The more powerful and attractive the vision, the more likely followers are to buy that vision and commit their personal energies to its realisation. But we also know from the study of social movements, that people are attracted initially by the picture created by the vision (story and narrative is hugely powerful here), but are sustained in their shared commitment through alignment of their values. Opposing ideologues often come together around a simply-expressed common purpose, but then rapidly fall out as their opposing motivations and values are exposed when they seek a deeper understanding of why that purpose is important, and how it should be delivered. The one force more destructive of a powerful vision than conflicting values is lack of sincerity or authenticity. Values must be lived and breathed!

This understanding leads us to the first of our considerations of leadership – principles that, if followed, contribute to successful outcomes in the world of the extended enterprise or whole system.

In the new world of the extended enterprise, the foundations for success are built on clarity of a graphically illustrated vision, and the alignment of explicitly declared values that are constantly reinforced in the way leaders live and breath them in practice.

The economic crisis triggered in 2007/8 marked a watershed that highlighted the dangers of a complex, interconnected set of systems in a rather dramatic way. The majority of observers interpret the multiple failings as weaknesses in an otherwise well behaved set of global structures. Eliminate the weaknesses and all will be well! Consequently, the world of corporate governance, regulation and risk management is increasingly focused on strengthening the rigour of controls in a renewed attempt to regain command of the logically, deterministic, Newtonian system.

But the globally interconnected world behaves as a complex adaptive system in which a few key elements of understanding indicate that such regulatory intentions are more likely to exacerbate, rather than prevent failure. The historical development of corporate governance provides an interesting study. Each new extension of regulation was triggered by a major catastrophic system-wide failing, where each such failure was usually triggered within a single organisation. Occasionally the trigger arose from complacency, ignorance or naivety, but more often by corruption or sustained efforts to gain new competitive advantage by stretching the boundaries of acceptability. But the catastrophic failures that led to wholesale damage arose when this attitude was accompanied by blindness and complicity in the governance fabric of the whole system (Maxwell, Enron, Lehman etc.).

Despite the fact that the quality of governance is invariably measured by process and task, experience tells us that failure is invariably precipitated by inappropriate behaviours or breakdown of relationships. This is true whether it be one of these major systemic failures, or simply a local organisational failure. The regulatory response to each has been to wrap increasingly complex compliance mechanisms across the system, each seeking to control processes and tasks. Concentration on a regime focused on enforcing compliance stifles the sense of ownership, constrains the initiative of individuals and teams, and suppresses innovation and quality improvement – the very elements that fuel sustained success.

In his review of the financial service industry collapse, David Walker[9] identified this reality:

….Board conformity with laid down procedures such as those for enhanced risk oversight will not alone provide better corporate governance overall if the chairman is weak, if the composition and dynamic of the board is inadequate and if there is unsatisfactory or no engagement with major owners……Principal deficiencies in boards related much more to patterns of behaviour than to organisation……

Similarly In her review of the safeguarding of children following several high profile and catastrophic failures, Prof Eileen Munro[10] identified precisely the same overburdening emphasis on process as a growing bureaucracy that inhibited the very purpose it sought to protect, stifling the care workers' ability to support the people in their care, commenting:

A move from a compliance to a learning culture will require those working in child protection to be given more scope to exercise professional judgment in deciding how best to help children and their families……. forces have come together to create a defensive system that puts so much emphasis on procedures and recording that insufficient attention is given to developing and supporting the expertise to work effectively with children, young people and families.

We have published the findings of our research3,[11-15] into the characteristics of effective leadership and how it needs to differ in the context of whole systems rather than single organisations. This reinforces these messages by stressing the importance of valuing and encouraging curiosity, because an effective complex system is one in which the widest possible view of learning is engendered. We characterise this as:

- adopting an open, enquiring mindset that is never satisfied it has found all the appropriate answers, looked far enough over the horizon to find helpful ideas from elsewhere;
- going out of your way to make new connections because each new connection opens up new possibilities, new ideas and new perspectives;
- viewing diversity in the widest possible context (different cultures, educational backgrounds, disciplines, ways of thinking, experiences, as well as the usual gender, ethnicity, sexuality, faith) and drawing deeply on these different perspectives that help shed new and creative light on traditional problems.

Such curiosity is a more powerful ingredient of good governance than a compliance culture. The high performing board sees itself as the first line of regulation for its business, values true diversity and constantly asks itself how it can improve. This demands an outward focus, searching for ideas and examples from which to learn, and a self-awareness stimulated by regular reflection on its own behaviours and effectiveness. By setting this tone at the top, such a board will foster product and/or service innovation throughout the organisation. For those involved in complex systems, innovation in both the business model and the critical relationships and interdependences across the system will be important.

Echoing these three dimensions of curiosity, research[16-17] shows that diffusion of innovation, (crucial to system-wide change) relies on three agents:

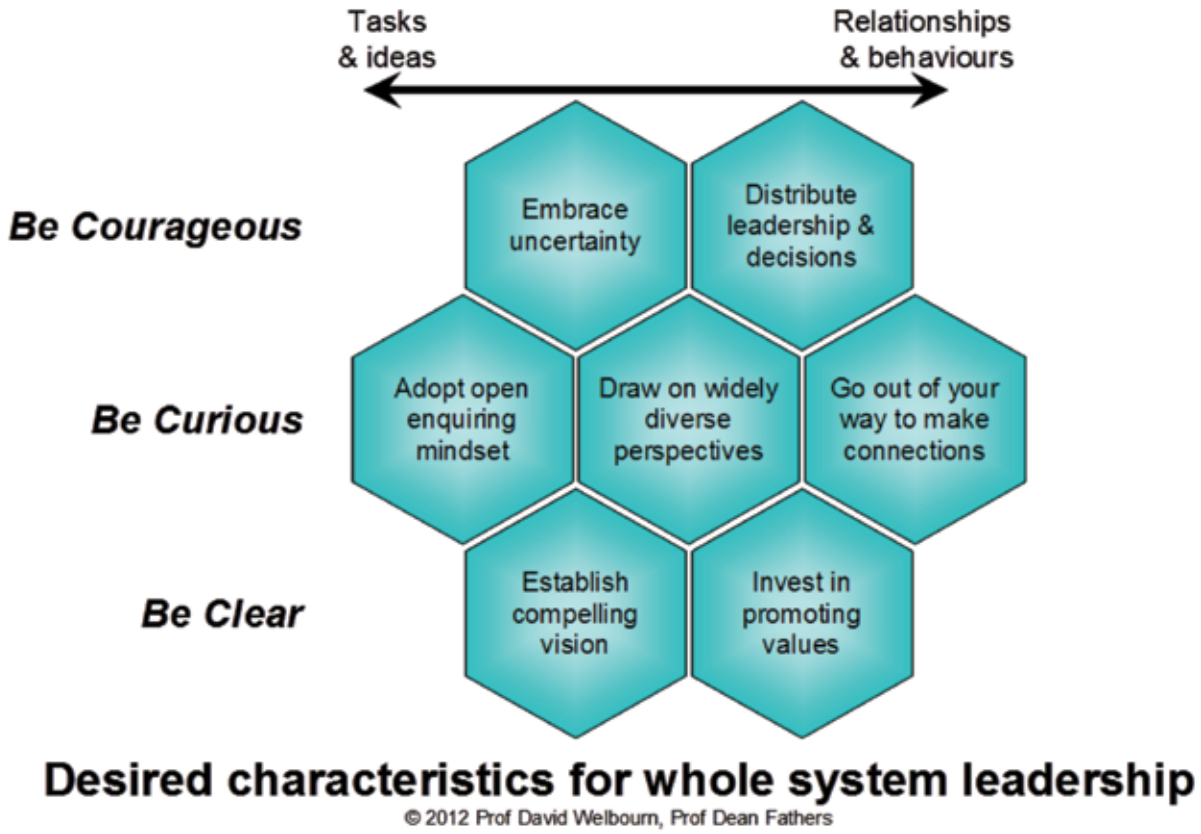


Figure 3.1: Desired characteristics for whole system leadership.

- mavens who have both access to knowledge and the insight to broker the right knowledge in the right time and place;
- salesmen who have the power to persuade others and build momentum;
- connectors who have the networks and connections to know who to engage with and how to build the right bridges.

Successful leaders of complex systems exhibit a heightened sense of curiosity that simultaneously seeks new knowledge and new relationships from as diverse a variety of contexts as possible, creating an environment that becomes embedded in the psyche of the system.

The final tier of our leadership model builds on the foundation of **clarity** and authenticity of both vision and values, and takes advantage of the fruits of **curiosity** to demonstrate **courage** in both its actions and behaviours.

A key element of this courage is to embrace the reality that uncertainty is a defining element of the system. This uncertainty will appear in all of the dimensions of VUCA and may manifest as both chaos and paradox. It is often experienced as a series of interconnected wicked problems for which there is limited experience on which to draw, whilst attempts at logical analysis prove to be frustrating and futile[18]. Wicked problems are like a water bed – apply pressure in one area and its effect manifests somewhere else. Wicked problems cannot be compartmentalised and solved in parts. They can only be addressed as a whole. They cannot be addressed superficially, they need deep understanding! They cannot be solved by individuals whose limited compass reveals only partial understanding, only by the diverse teams that can bring their varied experiences and multicoloured curiosity to bear.

The system leader must have the courage to face down these wicked problems, by throwing away the traditional rule-book. Harnessing the energy of conflict is demonstrated to stimulate more constructive approaches either compromising or avoiding such conflict. "Cooking the conflict" is an approach that openly embraces and works with the tensions of disagreement. The culinary metaphor is no accident – allowing the dish to simmer enhances the flavours, generating a more palatable outcome, but only when the conditions are just right. Too much heat risks destroying the flavour whilst too little reduction leaves the dish watery and insipid. Wicked problems demand a similar "goldilocks" approach, and leaders must combine their judgement and experience to know when it is "just right". This demands an ability to navigate at just the right combination of depth and breadth! They need to engage the subject at depth with a widely diverse team who have both the detailed operational knowledge and the breadth of influence to take and implement bold decisions. Such an approach is contrary to a typically expedient approach to problems that can too frequently be satisfied with a superficial understanding. It is also considerably more demanding of both time and resource, but it is the only way to find sustainable solutions to wicked problems. One senior leader commenting on such an immersive approach described it as "life changing" (See case study 2 - Total Place).

It is instructive to note that the beloved Pareto rule fails miserably when applied to complex systems. Over the long term, it is always the minor perturbation that creates the step change – never the mainstream. Conventional wisdom would seek solutions based on the prevailing climate, but it is the extremes of weather that create the turbulence wherein the risks really manifest. The hurricane or typhoon grows from a small anomalous wind pattern, reinforced over time by the feedback mechanisms created by the earth's rotation. Solutions that are both resilient and robust must anticipate the unexpected and unpredictable anomalies, rather than assume that designing to typical mainstream conditions will be adequate. In this regime, uncertainty dominates risk in the governance process, as the quantifiable is overshadowed by the unknown and unknowable.

The other dimension of the leaders' courage is the willingness to cede rather than tighten control[19-20], just when the risks and uncertainties are rising. The system can only gain the speed and agility to maintain resilience if the power to decide is vested in those with first hand knowledge who also have the ability for timely response. Leadership and decision-making must be distributed throughout the organisation and even wider into the extended enterprise or system. Much of the academic learning in this context has been derived from studying ant colonies whose behaviour exemplifies the art of decision-making that is truly distributed throughout the whole colony[21]. The collective decision emerges when the local information gathered by each ant is shared according to a set of rules that is understood across the whole colony. In practice, the Internet Protocol (IP) networks, instrumental in the working of the internet, are the largest human manifestation of such distributed decision-making. Each data packet contains header information whose interpretation at each node within the network determines which direction is the most favourable at that moment to ensure that the packet reaches its final destination. Communications within this intelligent

network are simultaneously cheaper, faster and more effective than the old point-to-point command and control systems they replaced. We are slowly realising this applies to organisational science too.

Whilst it may seem courageous of leaders to delegate responsibility throughout their own organisation over whom they can still exert authority and retain some sense of accountability, a clear mark of systems leadership is that of ceding power to others for the greater good, even where that is to another part of the system entirely. For this to work effectively, the whole system needs to develop an authorising environment[23-24] within which actors share a common interpretation of words, meanings, rules, norms behaviours and expectations. In short a process of governance that reaches across the extended enterprise, working in partnership with the governance operating within each of the discrete organisations or parts of the system. Unlike its single-entity counterpart, such an authorising regime is much more likely to be built on shared values than processes and protocols. An authorising environment will always exist. Even where it has not been intentionally formulated there will always be "the way we do stuff here", however informally it is documented or understood by all the players. It may often run counter to the formally agreed mechanisms. Failure to recognise the significance of an authorising environment will ultimately pose a severe limitation on the system, as it develops a level of exclusivity that is the preserve of those with the right connections, tacit knowledge, and appropriate back-door processes. The defining characteristic of such authorising environments is that they are not solely defined by structures and positional power, but are influenced by informal mechanisms built on respect, trust, credibility and situation.

General McChristal[22], in-theatre leader of allied forces in Afghanistan learned this from experience:

"We had to change our structure to become a network. We were required to act more quickly. Instead of decisions being made by people who were more senior – the assumption that senior means wiser – we found that the wisest decisions were usually made by those closest to the problem".

The wise system leader will expose these mechanisms to foster transparency and encourage inclusivity, and will seek to develop formal structures that run with the grain of the informal relationships wherever possible. In this context, effective system leadership is characterised by unusual descriptors: magnanimity, humility and servant leadership being important elements.

The final tier of system leadership is therefore characterised by courage – more than anything, the courage to rewrite the rule book of what matters in terms of personal behaviours, risk taking and the energy to face uncertainty by relying on others.

The systems leadership model shown in the figure below 3 and underpinned by published research, contains seven elements introduced above and repeated in the table below. These are split into the three tiers of clarity, curiosity and courage, and split laterally into those that focus on **task/process** and those that focus on **behaviour/relationships**. Achieving balance between the process-dominated "rational" world and the world of behaviours dominated by emotions, attitudes and beliefs is crucial to the new "quantum" science of the extended enterprise. It is appropriate that the relational model between these characteristics takes the form of a honeycomb, given the opportunity to learn from hive insects.

To emulate people who are successful in leading complex systems, the following seven approaches are recommended:

- go out of your way to make new connections
- adopt an open, enquiring mindset, refusing to be constrained by current horizons
- embrace uncertainty and be positive about change – adopt an entrepreneurial attitude
- draw on as many different perspectives as possible; diversity is non-optional
- ensure leadership and decision-making are distributed throughout all levels and functions
- establish a compelling vision which is shared by all partners in the whole system
- promote the importance of values – invest as much energy into relationships and behaviours as into delivering tasks.

The relationship between leadership and governance

So far we have focused on the combination of attitudes and actions that individuals need to adopt if they are to be successful in the most challenging aspects of leading across an extended enterprise or whole system. In any organisation, the most senior leaders will be the members of the governing body or board.

The governing body will be the vehicle through which governance is provided and this will inevitably mirror the collective characteristics of these most senior leaders. In the UK model of governance, the governing body comprises executive and non-executive members within a unitary relationship. Whatever differing perspectives have been addressed in the process of reaching a decision, once made, the final decision binds all its members individually and collectively to a corporate commitment. Internationally, alternative models include those typified by the US-style and the German style. The governing body in the US model is two-tier, separating the roles of executive and non-executive directors, so that external accountability is managed through the non-executive tier, who define the mandate within which the executive tier operates. The German model operates a unitary board similar to the UK model, but with the addition of a governing council of wider stakeholders (including workers) whom the unitary board must consult on all significant matters.

Whichever model is adopted, the governing body provides the contextual framework within which its members discharge the governance through their actions and decisions as leaders. We have already seen that leadership in the extended enterprise is founded on:

- the ability to establish clarity of purpose in which the importance of a clearly articulated vision and goals is reinforced by expressed values that are lived and breathed by senior leaders and therefore echoed throughout the extended enterprise;
- a curiosity that embraces the widest possible diversity, constantly seeks new sources of learning – both internal and external, and
- the courage to recognise that the volatility, uncertainty, complexity and ambiguity are part of the new reality that need to be embraced with the confidence and willingness to distribute decision making throughout the enterprise, even ceding power to others on occasions.

Earlier, we defined governance as the set of structures, processes and relationships within which decisions are made, resources deployed and accountability is managed to achieve agreed goals. It therefore follows that effective governance in the extended enterprise responds to these patterns of leadership, with a reasoned response to what occasionally appears counter-intuitive.

The most obvious response is that we can no longer view governance through the lens of process alone, despite the considerable weight of practice to this effect. Governance, whether weak or strong, is experienced in the attitudes, behaviours and relationships. In a predictable, Newtonian world, this can be expressed and measured through the proxy of the processes that support and measure these interactions. In this traditional world, the regulation of effective governance is dominated by compliance to the relevant codes of conduct[25]. Adherence to this code is designed to protect stakeholders including investors, employees, suppliers, from failure to exercise diligent levels of propriety and care towards their respective stakes.

In times of increasing complexity and VUCA, the temptation to strengthen controls and enforce compliance to rigid processes also grows, but we have seen through the lens of leadership that this is unhelpful. The relevant codes refer to "comply or explain", creating the opportunity for governing bodies to demonstrate (explain) why, after due scrutiny of the evidence and consideration of alternatives, they have exercised their collective judgement to reach a specific conclusion.

When facing rapidly changing environments which may impact their organisation both directly and/or indirectly via its extended supply chain or other partnerships, governing bodies may feel themselves under greater pressure to comply rather than to explain. But the real challenge to their governance arrangements is whether their approach is sufficiently agile to adapt to the uncertainty and volatility of the risks they face. The emphasis on governance therefore needs to focus on supporting resilience of the potentially complex partnerships and supply chain. The globalisation of markets and the speed with which the whole interconnected system adapts and responds to the numerous feedback loops introduces new and larger systemic risks and uncertainties, well beyond the reach and consideration of most decision-making. The horse meat contamination affair provides a perfect illustration of how a chain of policies and decisions created an unexpected vulnerability across an industry.

A governance approach should be adopted that helps supply chains to adapt and transform in response to new threats. This is in contrast to the traditional governance responses which lean towards seeking more control of the supply chain leading to increased costs and loss of supplier innovation.

The features of a resilient governance model are:

- governance focuses on the coordination of key relationships in the supply chain;

- new threats result in an increase in the flow of information and communication;
- whilst remaining commercially robust, power is balanced across participants within the extended supply chain;
- participants are empowered to try and resolve problems themselves, whilst providing transparency to other members;
- where new threats arise self-organising groups are encouraged to form to pursue solutions;
- governance encourages participant learning by accepting the inevitability of change and promoting experimentation;
- Participation of supply chain members is encouraged to build the trust and understanding needed to create self organising groups;
- Governance fosters a sense of joint accountability through equitable distribution of benefits.

The world of the extended enterprise is most simply characterised by its complex adaptive nature, and the combination of self-learning and self-awareness that this creates. Traditional emphases of management and governance have focused on processes that are essentially fixed. We have explored the need to shift the emphasis from management control to the empowerment created by a new style of leadership that is both inspiring and stretching. Models of governance are now following a similar pattern based on an expectation of constant learning and renewal – always striving to improve against an evolving base-line, and certainly not being satisfied with the concept of compliance, which is essentially passive.

The European Institute of Governance Awards (EIGA) has defined a model of governance that is underpinned by research evidence[26] It is built on a framework drawing on the self awareness and self learning of the governing body to ensure that it remains focused on the balance between creation of new value and protection of existing value, whilst assessing its overall impact – both declared through its goals and values,

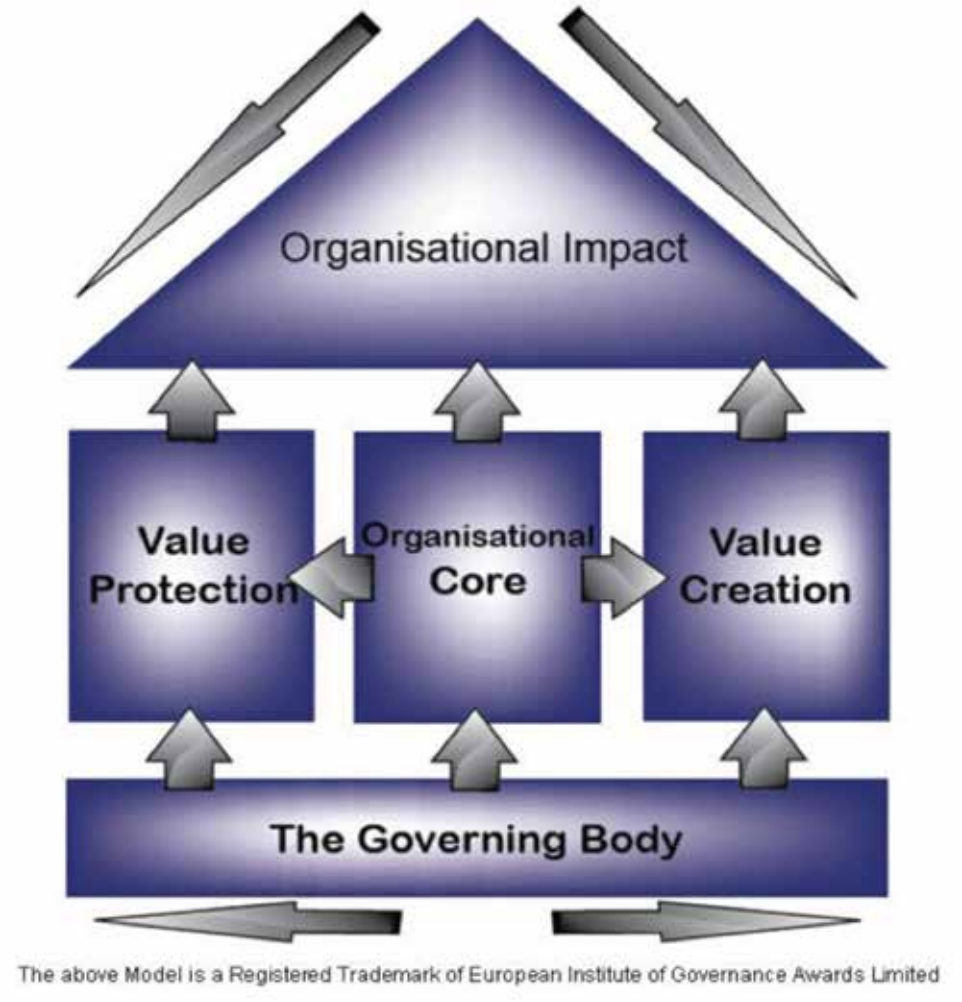


Figure 3.2: EIGA model of governance

and undeclared through its footprint. Unlike other standards-based approaches, this model offers a common framework as a reference for the effectiveness of governance to be independently benchmarked against the rising values and expectations of a demanding combination of markets and stakeholders.

Key messages from this chapter

When dealing with the extended enterprise, both leadership and governance need to focus on aspects of relationships that are driven by behaviours, attitudes and values, alongside the traditional focus on action and process. Invariably, poor outcomes, lack of success and failure of governance is more likely to emerge from ineffective relationships than from weak processes.

Most of our models of organisations, management and governance were developed from a "Newtonian" view of the world that was predictable and could be well understood. The high levels of interconnectivity, rapid communication and extensive feedback loops are more akin to a "quantum" view of the world that are complex and adaptive and characterised by volatility, uncertain, complexity and ambiguity (VUCA).

In this new paradigm, command and control environments are more likely to achieve perverse outcomes, and desired outcomes are more likely to be achieved through inspired leadership that uses influence and distributes decision making widely, to create greater agility, resilience and robustness with the power to adapt.

The key characteristics of this world are clarity of purpose, curiosity that supports constant learning, and courage to live with the complexity and to harness the energy that lies within conflicting ideas to fins new ways to deal with wicked problems.

Good governance cannot be imposed through compliance with standards, but needs to be constantly revised and improved by balancing good processes with wise judgement in a constant renewal process built on valuing diversity, developing self awareness and regular benchmarking.

References

1. Wheatley, M. J. Leadership and the New Science. (Berrett Koehler Publishers Inc.: San Francisco, 2006).
2. Wendell-Holmes, O. a distinguished Harvard medic, educator and pioneer - see profile in Wikipedia.
3. Welbourn, D., Warwick, R., Carnall, C. & Fathers, D. Leadership of whole systems. King's Fund (2012).
4. Ohanian, A. Leading in a VUCA world. Training Journal 19–23 (2012).
5. Euchner, J. Navigating the VUCA World - an interview with Bob Johansen. Research - Technology Management 10–15 (2013). doi:10.5437/08950308X5601003
6. Horney, N., Consulting, A., Pasmore, B. & O'Shea, T. Leadership Agility : A Business Imperative for a VUCA World. People & Strategy 33, 32–39 (2010).
7. Gleick, J Chaos, "The amazing science of the unpredictable" Vintage Books (1988)
8. Peter, L. J. Peter was an educator and management theorist who is best remembered for the Peter Principle - his assertion that in large organisations, people rise to their level of incompetence.
9. Walker, D. A review of corporate governance in UK banks and other financial industry entities. DTI publication (2009).
10. Munro, E. The Munro Review of Child Protection: Final Report A child-centred system. Department for Education report (2011).
11. Welbourn, D; Ghate, D; Lewis, J; Systems Leadership: exceptional leadership for exceptional times –Source paper 1 – Literature review, Virtual Staff College, October (2013) http://www.virtualstaffcollege.co.uk/dcs-leadership-provision/systems-leadership/the-literature/
12. Ghate, D; Lewis, J; Welbourn, D; Systems Leadership: exceptional leadership for exceptional times – Synthesis paper, *Virtual Staff College*, October 2013 http://www.virtualstaffcollege.co.uk/wp-content/uploads/VSC_Synthesis_complete.pdf

13. Lewis, J; Ghate, D; Welbourn, D; Systems Leadership: exceptional leadership for exceptional times –Source paper 2 – The views of system leaders, *Virtual Staff College*, October 2013 http://www.virtualstaffcollege.co.uk/wp-content/uploads/strategic_interviews_complete.pdf

14. Lewis, J; Welbourn, D; Ghate, D; Systems Leadership: exceptional leadership for exceptional times –Source paper 3 – UK leadership scenarios, *Virtual Staff College*, October 2013 http://www.virtualstaffcollege.co.uk/wp-content/uploads/leadership_scenarios_complete.pdf

15. Welbourn, D. Leadership of innovation in the NHS - a literature review of good practice. *Innovation health and Wealth* (Department of Health)

16. Davenport, B. Occupy Complexity: Using Complexity To Examine The Occupy Wall St. Movement... *Emergence: Complexity & Organization* 13, 87–93 (2011).

17. Keith Grint Wicked Problems and clumsy solutions: the role of leadership. *The new public leadership challenge* 169–186 (2010).

18. MacGillivray, A. Leadership in a network of communities: *The Learning Organisation* 17, 24–40 (2010).

19. McMullen, R. S. & Adobor, H. Bridge leadership: a case study of leadership in a bridging organization. *Leadership & Organization Development Journal* 32, 715–735 (2011).

20. Gordon, D. M. *Ant encounters: interaction networks and colony behaviour*. (Princeton Unversity Press: 2010).

21. McChristal, S. General Stanley McChristal held several commands in the US Army and was particularly known for straight talking. He was the Chief of US forces in Afghanistan.

22. Moore, M. H. Public value as the focus of strategy. *Australian Journal of Public Administration* 53, 94 (94AD).

23. Benington, J. Moore, N.H. (editors) Public value – Theory and practice, Palgrave Macmillan, (2011)

24. see for example the UK Corporate Governance Code published by the Financial Reporting Council, https://www.frc.org.uk/Our-Work/Codes-Standards/Corporate-governance/UK-Corporate-Governance-Code.aspx

25. European Institute for Governance Awards http://www.eiga.eu.com/

Chapter 4: Assurance for the extended enterprise

Richard Anderson

For any organisation the proof of the pudding for risk management is the knowledge that it can live and operate within the boundaries of its risk appetite and tolerance. Understanding an organisation's propensity to take risks is only part of the equation. The other side is understanding an organisation's propensity to exercise control. Under- and over-control both can have devastating impacts on an organisation and its ability to achieve its objectives. Both should factor in to its risk appetite and tolerance, and both should factor into its overall strategic intent, and should help to shape policy, procedures, transactions and the business model as a whole.

If that is the case for a standalone enterprise, how much more important it must me for the extended enterprise: do you know where the weaknesses are such that a single straw could break the camel's back? This in essence is the issue of assurance: how do directors know that what they are being told is happening, or will happen is indeed happening on the ground? For many organisations this is an accumulation of activities:

- Management provide reports;
- Some organisations use varying types of control or risk & control self-assessment reporting;
- The company issues reports to the outside world;
- Internal audit provides an "independent" view of activities, providing a review to management and the board;
- External auditors report on the financial accounts;
- In some industries regulators undertake reviews of specific activities;
- External consultants or assessors sometimes provide assurance about specific aspects of the operations or strategy of the company;
- Some businesses seek reassurance about their suppliers' activities.

In essence assurance is an accumulation of evidence from a varied set of sources of differing levels of independence. Taken together, the various sources of evidence can provide the board with a sense of comfort that things are operating as they expect. In a sense risk management is almost the font of assurance, because one of the keys to successful risk management is that it should be the disruptive intelligence that pierces perfect place arrogance. To the extent that boards remain confident in their activities even after all the disruptive questions have been asked, then there is potentially an even higher degree of confidence or assurance than existed beforehand.

The issue that we face with complexity in 21st Century organisations is that the levels of assurance for any one part of the extended virtual organisation rarely reach out beyond the boundaries of the organisation itself except in very specific and quite niche areas (for example some businesses insist on IT Security or Privacy reviews of key suppliers, others might insist on Quality Accreditation for certain suppliers) but these rarely give a comprehensive view of the activities of other participants in a full extended enterprise. Yet we know that many disastrous risk management failures, which ultimately impinge on one part of the virtual organisation frequently happen within the corporate environment of another organisation: one only has to think about the Macondo Well incident in the Gulf of Mexico or the Horsemeat scandal.

We think there are four main elements that make the assurance dimension much harder to establish in the extended enterprise:

1. **Complexity:** the extent to which we are dealing with simple or complex problems will determine how easy it is to develop a sense of assurance that operations are running acceptably. Simple problems are easily dealt with by means of expert reviews, either internally or externally. Complex problems are quite simply that: complex and are not as readily susceptible to review because of the emergent nature of problems as different activities are undertaken.
2. **Scope:** risk by its nature can run at a strategic, tactical or operational level. Assurance needs to be gained at the same levels. However, understanding the impact of a strategic risk in a distant partner in an extended enterprise on the achievement of your own objectives is at best difficult. Mechanisms for managing operational risk are relatively easier to establish.

3. **Span:** the further a risk event is from one part of an organisation to another, the harder it is to establish whether appropriate mechanisms are in place for managing risk.
4. **Coupling:** Close coupling is said to exist where each part of a process needs to be done to time and to appropriate quality standards in order to ensure that the overall objective is not jeopardised. On the other hand, where loose coupling exists, the exact order and timing will not be as important. Close coupling in extended enterprises is easy to establish by the establishment of appropriate specification, but a failure of close coupling in a geographically diverse virtual organisation is harder to manage.

In a world of complexity, with divergent strategic intent, enormous span and potentially wide ranging close coupling it is hard to imagine how traditional sources of assurance can operate:

- External audits of financial accounts have little or no relevance: accounts are ex-post indicators produced long after the event and deal with a comparatively restricted view of the organisation.
- Internal audit is by definition lacking in independence in the context of the extended enterprise, despite the IIA's mantra, simply because each internal audit team is employed by one, and only one, of the participants in the extended enterprise.
- Regulators in different countries can take radically different views, if for no other reason than the differences in the regulations they are being asked to oversee.
- Management reports are unlikely to reach out of the direct line of management control.
- Specialists are by definition only going to take one perspective of the issue.

We therefore are suggesting that we need to move from a paradigm of control over things that have happened to a paradigm of control over events that have not yet happened and where the size of impact and likelihood are uncertain: in other words assurance over risk management. We believe that there are three elements that need to be put in place in order for each board to begin to gain assurance:

1. There needs to be a **form of governance** that works for the extended enterprise. This requires clarity about the four key social dynamics:
   a) Relative power;
   b) Incentives (financial and non-financial);
   c) Regulatory environments; and
   d) Shared values.

   Without an expressly agreed form of governance, participating boards should remain wary.
2. **Risk management capability**, which in our guidance on risk appetite and tolerance we defined as being a function of (i) ***Capacity*** (how much you can carry?); and (ii) ***Maturity*** (how well can your people cope?), needs to be understood across the extended enterprise. The rationale being that if risk management capability is good across boundaries, then there is an expectation that control can be maintained across boundaries. If it is poor, then this is less likely and alternative mechanisms need to be established.
3. There needs to be a flow of appropriate **risk management data** between organisations, especially data relating to forward looking key risk indicators.

Developing assurance mechanisms that work will involve considerable effort, and is likely to require:

- General up-skilling of risk management across the extended enterprise;
- Mechanisms to review:
  - o Adherence to an agreed governance approach;
  - o risk management capability across participants in the extended enterprise; and
  - o Shared risk management data to ensure integrity and appropriate data governance standards are applied.
- Tools to facilitate the risk mapping across the extended enterprise.

We think that assurance will move to being more relationship-based and less transactional, more forward-looking and will involve more conversations in risk between all parties. This remains an area with considerable scope for development, and at IRM we are keen to work with other organisations to develop such an assurance framework for extended enterprises.

Chapter 5: Questions for the Board

Mike Morley-Fletcher, Louise Gravina, Jake Storey

The principles for risk management and Internal Control outlined in the UK Corporate Governance Code (and in other similar codes around the world) demand that the board should take responsibility for determining the nature and extend of the significant risks it is willing to take in achieving its strategic objectives. To support this, clarity over strategic objectives is critical to provide a context for understanding and identifying risks, associated risk appetite and the overall risk culture of the organisation. The UK Code further notes that the board should maintain sound risk management and internal control systems. To this end, it is important for the board also to understand

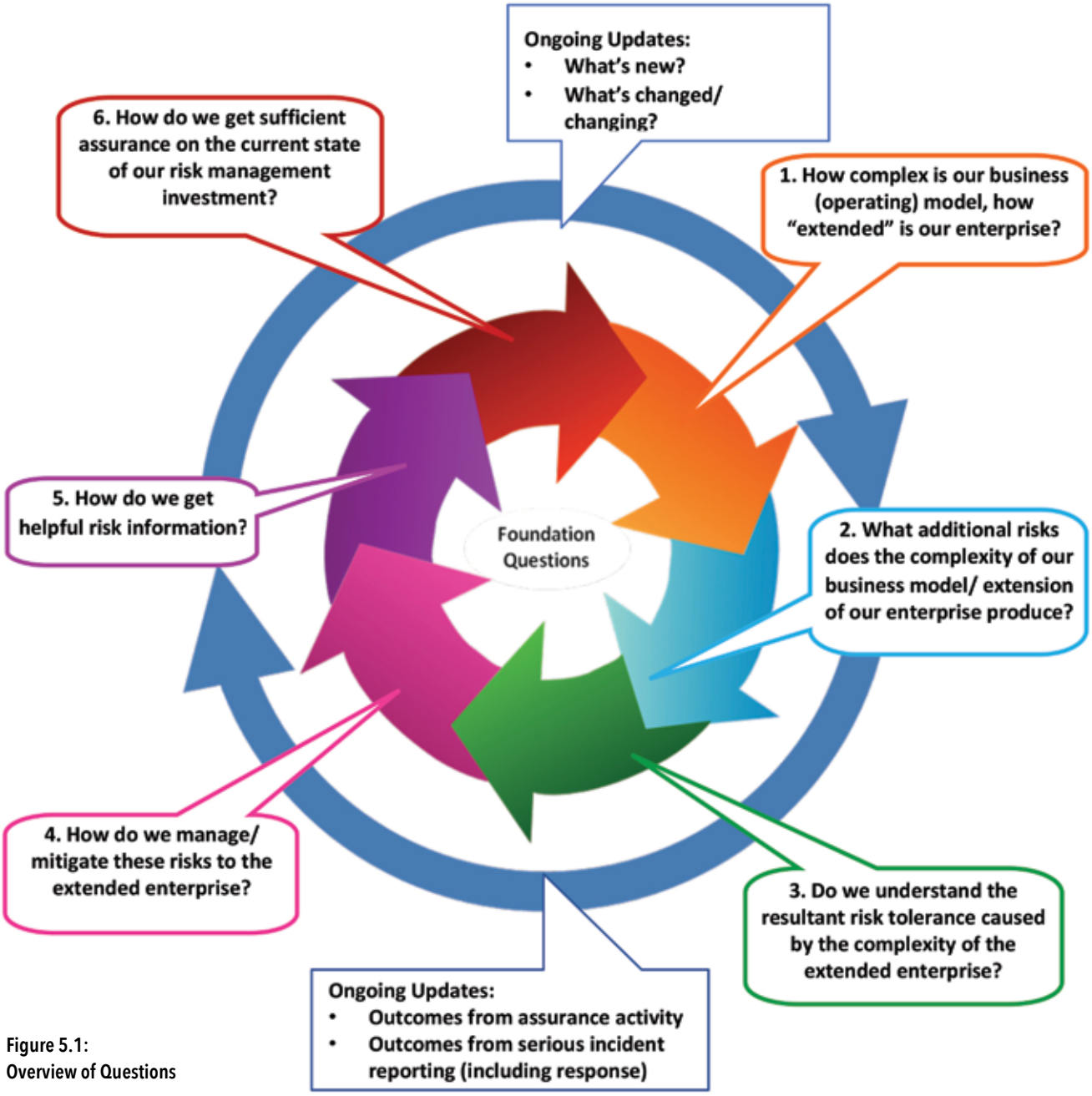


Figure 5.1:
Overview of Questions

the additional complexity and risks exposed by an extended enterprise analysis of the organisation. The board should seek to assure themselves that the system of risk management is designed in such a way that it considers this potential increased level of risk too.

In Figure 5.1 there is a series of questions for the board to enable challenge and drive understanding of where the key risks reside and how they are being managed and monitored, so that the board receives this fuller picture. The questions are divided into two categories:

- **Foundation** – appropriate for initial discussion and getting the risks associated with the complexity and extension of the enterprise onto the agenda.
- **Ongoing** – appropriate for maintaining visibility of risks and keeping informed of changes which have a significant impact on the risk landscape or risk exposure.

Where questions may be more suited to Non-Executive Directors – to help understand what needs to go right in order to support delivery of strategic objectives, what may affect the achievement of these objectives and where there is significant reputational risk exposure – these have been highlighted in italics.

Foundation questions

(Questions that Non-Executive Directors may want to ask are highlighted in italics)

1. How complex is our business (operating) model, how "extended" is our enterprise?

What is the extent of the complexity of our enterprise or our reliance on relationships with third parties?

How stretching are our objectives, targets and purpose? Has this changed?

What are our business model's key (critical) processes, functions?

What are the strengths of its design, what are the weaknesses?

What are the strengths of how it is operated, what are the weaknesses?

What are the key decision points in operating our business model? Where are decisions made (centralised v decentralised, own v third party)?

What is changing in our business model that could produce changes in the nature and / or extent of risk to our enterprise?

Who has accountability for ongoing management of the extended enterprise? Where have we delegated responsibility to third parties?

2. What additional risks may the complexity of our business model/ extension of our enterprise produce?

Which specific risks will be exacerbated by an increase in the complexity of our business model/ the extension of our enterprise?

- What level of risk analysis was conducted when changing the business model? Additional complexity to the business model is likely to exacerbate the nature and extent of risks. Do we use a risk Universe for completeness checking?
- New or enhanced risks from extending the enterprise might include:
  - Legal and regulatory responsibilities, e.g. bribery and corruption, anti-money laundering
  - Supply chain integrity, e.g. traceability, quality, employee welfare, sub-contracting
  - IT capability, e.g. outsourcing, cyber attack
  - Brand integrity, e.g. franchising, joint ventures, licensing, sales force
  - Corporate reputation, e.g. when outsourcing operations we may be able to protect ourselves from financial loss, but much harder to avoid reputational damage

Where are the resultant "single points of failure" in our more complex/ extended enterprise?

- Which key (critical) components, processes, functions, people could, if they fail, significantly curtail or stop our enterprise from operating?
- Have we conducted a thorough analysis of "single points of failure", "choke points"? Do we know where all of them are?
- Which of these do not have easily accessible substitutes?

What are the "systemic risks" for the more complex/ extended enterprise?

- Which events/ scenarios could trigger a combination of reactions that could cause widespread damage to our enterprise?
- Have we conducted a thorough analysis of "systemic risk" scenarios? This should be in addition to looking at risks on an individual basis
- What are the critical inter-linkages or dependencies in our enterprise, where the failure of a single component, or cluster of components,

3. Do we understand the resultant risk tolerance caused by the complexity of the extended enterprise?

Can we get a true articulation of our risk tolerance in areas of the extended enterprise that we don't control and how might we express that?

- What are our tolerances/ appetite for risk in the extended enterprise? How well understood is this? How clearly articulated? When can we measure it? When can't we measure it? Financial v non-financial, other things that matter to our stakeholders? What about in areas of the extended enterprise that we don't control?
- Is our resultant tolerance/ appetite for risk reflected in the rate of return expected and extent of risk management and contingency needed? "Are we getting a commensurate reward for this additional risk we are taking?"
- Do we understand our tolerance for individual risks AND for the systemic risks from a combination of risk events?
- How resilient is our reputation to issues caused by the complexity of the extended enterprise?

Have controls for all key decisions (decision points) in operating our business model been covered?

- What are the key controls embedded in the design of our business model to manage the resultant risk exposure to our agreed risk tolerance?
- What are the key controls in the operation of our business model to manage real time the resultant risk exposure to our agreed risk tolerance?
- Which risk mitigations are within our control and which are with third parties? Of those with third parties, how strong is the enterprise's influence over the performance of these controls by the third party and where is it a matter of "trust"?
- Are there appropriate mitigation plans to reduce the likelihood of a failure at a critical "choke point"? How many of these are within our control?
- Are there appropriate mitigation plans to reduce the likelihood of systemic risks? How many of these are within our direct control?

How do we contingency plan for catastrophic events?

- Have we conducted a thorough analysis of our contingency plans? Are all required plans in place?
- Which plans are within our control and which are with third parties? What additional measures can be put in place to improve our "ownership" of all our key contingency plans?
- Have individual plans in the extended enterprise been reviewed on a systemic basis to identify pinch points on resources, gaps in coverage and conflicts between different plans, so that "co-ordination" protocols can be designed?
- *Have plans been rehearsed (for capability and coverage) and linked into crisis management capability? How is this established for contingency plans owned / operated by third parties?*

5. How do we get helpful risk information?

What risk information is needed to (i) protect; and (ii) grow the enterprise?

- What is needed on an ongoing basis (monthly, quarterly), and what is needed to support specific investment decisions?
- Are key risk indicators ("KRI") used to measure changes in the nature and / or extent of our enterprise's risk profile, in comparison to our risk tolerance/ appetite, and so warn of impending risk events?
- Are key control indicators ("KCI") used to measure the effectiveness of controls existence and operation and to warn of control weaknesses or failures?
- Has our enterprise's various sources of reporting on risk and control been combined to provide senior management with a single dashboard? Is it clear who deals with which issues?
- *Is this information (KRIs and KCIs) integrated into our enterprise's performance management system / dashboard of key performance indicators ("KPIs") to provide warning of impending issues and / or reassurance of sustainable performance?*

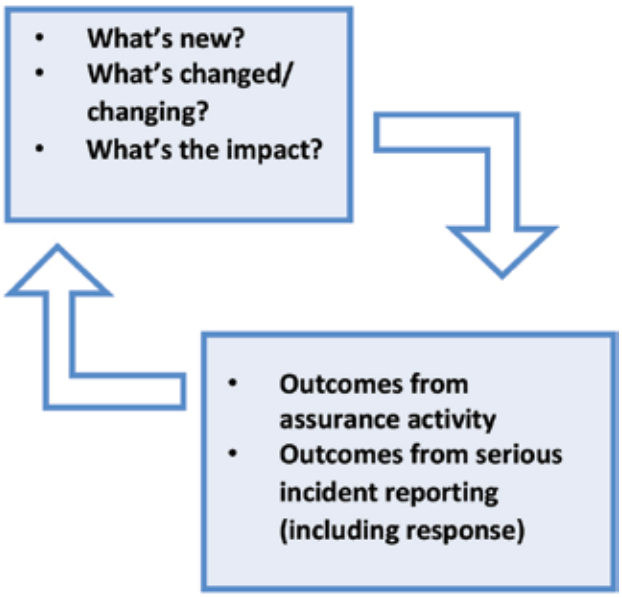
6. How do we get sufficient assurance on the current state of our risk management investment?

Have we conducted a thorough analysis of our assurance needs?

- *Do we use an Assurance Map for completeness?*
- Which assurance mechanisms are within the enterprise's control and which are with third parties?
- Of those with third parties, how strong is the enterprise's influence over the performance of these assurance mechanisms by the third party and where is this a matter of "trust"? What additional measures can be put in place to improve the enterprise's "ownership" of all the assurance mechanisms it needs to rely upon?
- *How effectively and consistency have sources of assurance (functions, activities, reporting), the "third line of defence", been aligned, co-ordinated and integrated?*

Ongoing updates

Raising the board's awareness of the risks that present themselves in the environment and relationships which extend beyond the enterprise in such a way that is simple and clear can present a real challenge given the potential degree of complexity. The right questions asked to the right people at the right time will help ensure the board has the information required to support decision making and appropriate challenge of management. These will include questions as the changes start to happen, and then others as the change continues:



Some final questions

At its simplest, as an organisation becomes more complex and/ or extends its enterprise, the board will have three key questions to understand its risk exposure:

- Has the board been updated on the risks introduced by virtue of changes in complexity and an extended view of the enterprise?
- How has this impacted the board's risk tolerance/ appetite?
- How does the board receive appropriate assurance, e.g. per time, cost, quality and objectivity, that these increased risk exposures are within the tolerance/ appetite set?

Chapter 6: Building trust across an extended enterprise

Peter Neville Lewis MIRM

"Risk is as much about people as about anything else. Risk management is most likely to fail when the human element has not been taken into sufficient consideration. The challenge is to measure all the non-numeric elements, all those that have an impact on an individual's behaviour.

Stop thinking of business as something mechanical – business is about people, a complete eco-system where all things are connected to each other. The human dimension is essential when assessing, communicating, managing and advising upon risk.

Anthony Hilton (Financial Editor of the London Evening Standard speaking at an IRM event in 2012)

Introduction

In this chapter we consider the view that systems, process, regulation etc. (call it "box ticking" if you will) can never hope to manage or control the idiosyncratic behaviour of individuals confronted with uncertainties, lack of experience, inadequate knowledge or information, and temptations to do the wrong thing.

Risk management is really a misnomer. Organisations need to be more risk "intelligent" tracking forward all eventualities and monitoring how people are responding and could react. (See the final sentence in Anthony Hilton's quote above.) How will they behave in confronting these challenges?

Handling externalities is how trust is built over a period of time. How people make and take decisions determines overall culture.

Trust comes from the right behaviours under pressure. And the example for these behaviours comes from courageous leadership with integrity.

Overview

Every organisation needs to be explicit about who they are and why they exist.

Every individual needs to understand their character and purpose.

Understanding how and why decisions are taken is central to managing risk – internally and externally.

Actions and behaviours, guided by the leaders, should send an unequivocal message to all who interact with the organisation that it knows its purpose and will never compromise its standards, ethics and way of operating.

This is why an organisation's Moral Compass© (see diagram below) is absolutely central to its existence.

It guides strategy, operation, people and performance.

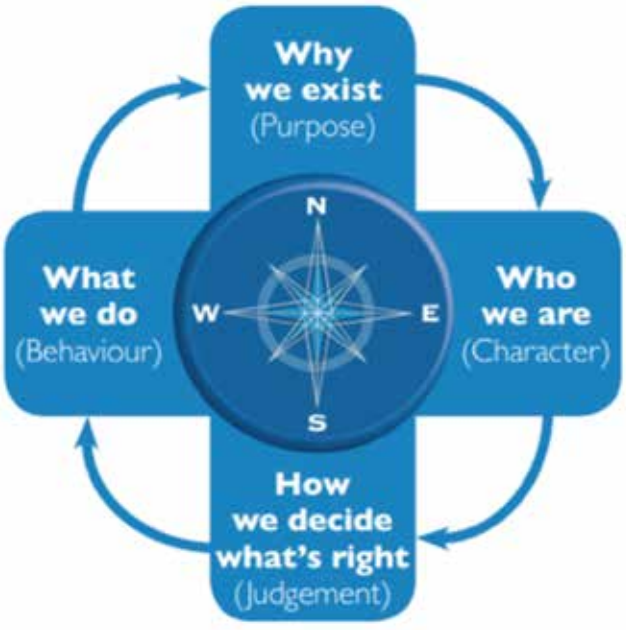


Figure 6.1 Moral Compass

An organisation that takes the time to really understand its true purpose and how it can be of service to the society which grants its "licence to operate" will by default add value to its self, earn respect for what it does and build trust with all its stakeholders.

Organisations with such a profile and values will have a better chance of managing their own known risks, dealing with the uncertainties of unidentified risks and combating and avoiding contamination from organisations who do not meet the same high moral standards.

Is risk appetite aligned with values and behaviours? Are open and frank listening conversations taking

place at all levels of the organisation? Does somebody know something? (NB There were clues about the 9/11 disaster, it now appears).

We must never be complacent and must recognise that societal expectations are a moving target. Current best practice could be tomorrow's derogatory headlines. 30 years ago workplace deaths in heavy industry were common place – now the bar is set at zero tolerance. Ongoing moral vigilance is essential to mitigate reputational risk. Effective ERM means the courage to sense when something might be wrong and take unpalatable decisions.

Personal risk management

Managing and mitigating risk should not be difficult provided everyone involved knows what is expected of them and is committed to doing their best to deliver on this.

There is a very simple model which covers many of the basic requirements – let's call them the 3 D's.

Duty. Know what you are supposed to do, understand what is required and fulfil your obligation. Have a duty of care.

Discipline. Stay in control of yourself and your work, manage your emotions and do not allow yourself to be distracted or tempted by people or events outside your duty. Remain focused.

Delivery. Make sure you keep your promises, always do what you say you will do in a dutiful and disciplined way. And if you cannot, then you need to re-contract - that is acceptable if it is done openly and consensually.

You could describe the above model as Acting with Integrity, doing the right thing in the right way (even when nobody is looking) plus adhering to key universal moral values.

If everybody behaved like this and observed the rules of the game, we would clearly not have so many challenges in how life and business get played out.

The outcome of doing things right is that trust is engendered. Trust at its most powerful means a complete belief in a third person. Trust like Love has to be given and received and it is this reciprocity (or lack of) that should create a special relationship between organisations and between the individuals within them. Trust also helps to create openness and transparency, another key factor when it comes to managing organisational risk. All the rules in the world cannot replace trust based contracts where values are honoured and respected.

But all the above is largely focused on individual or group behaviour. However well-intentioned people may be, there are inevitably others in the world who have a different code, or who choose to break or ignore the codes which groups of people agree on as the way they would like to interact with each other in the various spheres of life.

And so doubts creep in. Once we cannot be sure how other people are going to behave, uncertainties arise and this is where risk manifests itself. Trust is "at risk". We can no longer manage what we do not know or cannot reasonably anticipate. At the next level of risk we then have to ask ourselves the much harder questions – to start thinking the unthinkable relative to both internal and external shareholders.

What is it that we might not know?

Have we consulted widely enough to cover every conceivable risk factor?

What might happen that is almost impossible to imagine (Black Swans)?

Poor decisions

Why do things go wrong? Because people a) do not do what is expected or b) they do what is not expected! In both cases there is a common factor - the making and taking of a decision.

So is it possible to determine a decision framework which would help to c) do what is expected? The answer is a tentative "Yes", but it would require the moral training of all the planet's inhabitants! Clearly this is an impossibility and therefore ignoring or bypassing even a handful of the world's citizens leaves the world and its inhabitants at permanent risk.

For example, it only needs a small number of corrupt farmers, growers and food producers to collude in order to contaminate the global food supply chain.

We are all aware of examples of this happening, so what are the remedial steps to prevent re-occurrence?

Rotten apples

The fundamental problem for ERM is that anyone (yes, one) person is bigger than the system. Think Nick Leeson (Baring Bros), Kweku Adoboli (UBS). Jerome Kerviel (Societe Generale) – all lone operators who circumvented sophisticated internal audit, control and supervision.

Read the Airmic report Roads to Ruin and you will realise that senior executives, in many cases failed to see or listen to clear evidence that trouble was in the offing.

And again in certain instances - AIG (Hank Greenberg), Enron (Kenneth Lay), Independent Assurance (Michael Bright), Northern Rock (Adam Applegarth) key individuals simply overrode the system – illegally, recklessly and unchallenged.

At times they were driven by greed (or lack of discipline), at others by hubris and arrogance (lack of humility). We need look no further than RBS and Fred Goodwin. The FSA Turner Report makes the comment that it was a failing of culture as much as anything which caused RBS's downfall.

Human weakness

The crucial point to be made is that in nearly all negative risk events, either an individual or a small group has made either a sub-optimal decision, or not made the decision which might have mitigated the eventual outcome.

Margaret Heffernan's excellent book, Wilful Blindness provides numerous examples of this type of behaviour and suggests that human beings may even be programmed to avoid awkward decisions or take safety in numbers. Constructive challenge at all levels in an organisation is therefore a healthy counterpoint to overcoming blind spots.

A culture of integrity

What then is required to create an environment where risk events are less likely to happen?

The solution put forward by many thought leaders is that the culture of an organisation can be the defining factor. The word culture comes from the Latin cultus meaning root and implies growth through cultivation of relationships and resources.

It may be helpful to enlarge on this by calling it a culture of integrity. Culture is the aggregated and mutually agreed sum total of all the behaviours of a group of individuals. Integrity is the aggregate of those core values (Moderation, Empathy, Trust, Humility, Excellence etc) which exercised together make up our moral DNA. Initially this cultural group will have a small number of founding members but others may and will be attracted by what they stand for and how they behave ("how we do things round here") to form larger cultural groups, tribes or nations.

Behaviours are actions which, repeated, become habits. Actions or acts are the outcomes of decision taking, preceded by decision making.

Judgement is what we exercise when we make decisions.

Character is what we use subconsciously or cognitively to inform these judgements. NB Each of us is a unique individual with our own principles and personality and we can, and often do, arrive at different judgements even in similar circumstances.

Values are the building blocks of our character. They are core to our humanity and include Love, Courage, Fairness, Humility, Self-Discipline, Excellence etc., all part of what Aristotle described in his Nicomachaean Ethics (c350BC) as virtue ethics

Measuring organisational culture

So, to recapitulate, organisations need to be 100% clear about what their values are, what they truly mean to the people who work there, and what behaviours are expected of them. Clarifying these values and measuring their internal effectiveness is a tricky task, but there is a well validated psychometric tool called MoralDNA™, which has been used successfully for the last 5 years to track both individual and organisational culture. The results can be reported in simple graphic formats which are easily understood.

What MoralDNA™ reveals, almost without exception, is that particularly in respect of the values of Empathy, Humility and Self Discipline, those in senior positions do not score as highly as the average workplace population. These values relate to what is known as Ethic of Care. For executives in an organisation to be lacking in the above means that they are prone to care-lessness and are not care-ful. Both conditions are natural precursors to poor risk management.

An even bigger worry is that these findings are based on how people report at work but when asked about the above values in their home lives there is a marked improvement. This is a common finding with almost all MoralDNA™ surveys across all levels of an organisation.

So the conclusion has to be that decent people are often not bringing their full selves to the workplace. Or, they are not expressing their truer self. Is that due to organisational influence and pressure? There are strong grounds for suspecting this since we also know from MoralDNA™ feedback that organisations have a strong Ethic of Obedience – in other words they focus on rules and compliance which inevitably creates a culture of fear, conformity and lack of creativity. All of which leads to frustration, tension, and eventually anger.

MoralDNA™ and decisions

Decisions are driven, many philosophers have reasoned, by four factors:

EGO: the least attractive part of our human condition which if not managed and controlled by our personal values can develop into sociopathic or even psychopathic behaviour.

OBEDIENCE: staying within a social framework which, if not agreed by all, will either be rigorously enforced or eventually circumvented.

REASON: the experience, wisdom, emotions and context which enable us to try and do the right thing and, if necessary, over-ride the rules.

CARE: the most powerful of all human emotions and ethical consciences. It enables our long term survival as a species and is the glue in our societies. And yet MoralDNA™ research pinpoints that it is sadly lacking in many organisations. Care-less decisions usually have only one outcome!

MoralDNA™ measures three of these:

Obedience - covering rules and compliance

Reason - covering wisdom, experience and emotions,

Care - covering love, empathy and compassion

These three *ethical consciences* are key to how we handle our ego, the prime driver of basic human survival (as well as greed, impatience and poor discipline), which, as those who have had young children will testify, can be unattractive at times in its self centredness and is hard to manage.

We need to hold these consciences in a reasonable equilibrium if we are to make and take sensible decisions.

Figure 6.2 below shows that there are nearly always significant negative differences between the moral values and ethical consciences people draw on in their personal lives and those that influence their decisions and behaviours in the workplace. The consequence is that organisational cultures are flawed with damaging effects on risk management and reputational protection.

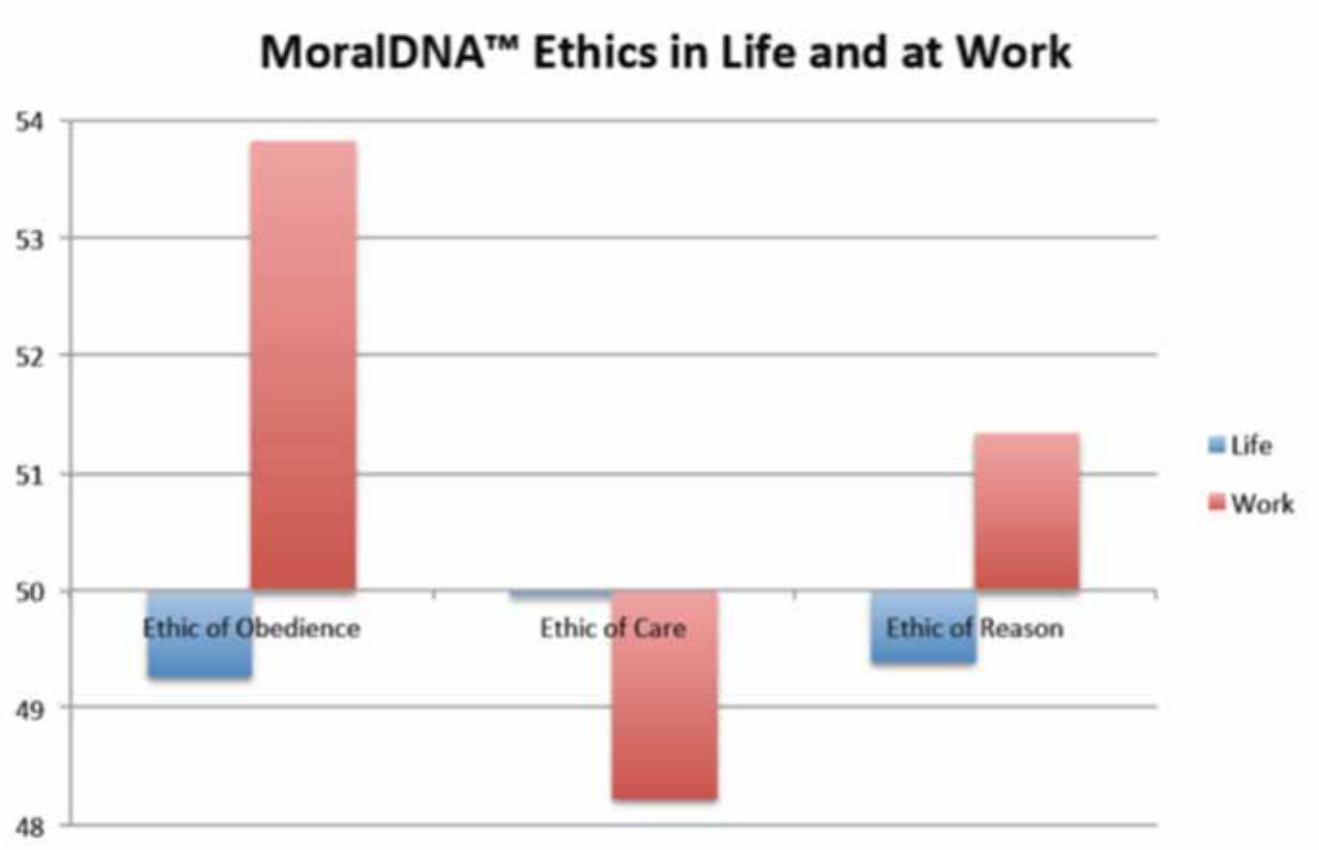


Figure 6.2 MoralDNA EthicsTM in Life and at Work

Controlling risk supports sustainability

There is a huge amount of psychological and behavioural work to be done in many companies if they are to survive and evolve into caring organisations whose cultures permeate all with whom they interact. Efficient management practice will take them so far but the behavioural evidence for risk avoidance and thus sustainability is reasonably clear.

There are respected companies who do operate with a high ethic of care and concern for all their stakeholders, most notably:

John Lewis Partnership (UK) - 1928

Unipart (UK) - 1987

W L Gore (USA) - 1958

Ocean Spray (USA) - 1930

South West Airlines (USA) - 1967

Mondragon (Spain) - 1956

Tata Industries (India) - 1868

Interestingly these organisations have avoided scandals and stood the test of time (see founding dates) rather well and their corporate logos do not adorn the Hall of Shame which features so many well known names from the BBC to Barclays, BP, RBS, Serco, Tesco, etc. etc. Why? Possibly because, in the words of South West CE Herb Kelleher, "*if you create an environment where people truly participate you don't need control. People know what needs to be done and they just do it.*"

Managing risk holistically

Values, Behaviours and Culture are core determinants of what an organisation stands for and what its moral purpose is.

This must be the bedrock from which it operates. It must be exemplified by all senior management, who should also be psychologically profiled to identify any potential character weaknesses.

The Board, senior leaders and operational managers have to live, breathe and evangelise decency and right minded behaviour so that every member of an organisation is in no doubt as to what is expected of them. Their personal commitment, in writing should also be obtained. Engagement with values and their associated behaviours is crucial.

(NB John Lewis Partnership could for example be said to have c87, 000 risk managers – their entire workforce!).

Identifying and eradicating the "rotten apples" is a daily ongoing task for everyone at all levels and requires a transparent speak-up policy re-enforced at Board level. Wrong doing cannot be condoned as it leads inevitably to fudging, corruption and a deterioration of standards. Risk avoidance then becomes so much more difficult to control. There has to be a high degree of risk awareness at every level. (The anecdotal evidence from the BP Texas City disaster was that plenty of BP employees knew that the site was a potential death trap but nobody in management wanted to hear the message).

Power and weakness of organisational culture

Organisations with a strong collaborative culture are less likely to be open to potential risk. Their best practise and attitude to risk will transfer to third parties and sub-contractors who contribute to these organisations' growth.

Discouraging open conversations on the other hand can only lead to hidden truths and non-disclosures of potential cultural information. Silo-isation between competitive teams, divisions and even regions may encourage information retention.

People must be able to raise issues and this practice should become part of weekly or monthly meetings. This "news from the front" may at times seem trivial, but listening and observation, connecting the dots and making intelligent deductions are vital components in the hunt for hidden risks. Risk "intelligence" is more important than risk management and risk registers!

A plethora of rules (often considered petty) is a sure sign that a proper open culture is not in place.

A classic case is the NHS whose systems, targeting and over-management are so interfering and ultimately counter-productive that the very thing they most exist for - providing care for patients - can become marginalised and at times even circumvented.

Failure to create the right culture within some units of the NHS has led to catastrophic consequences and these are classic but desperately sad examples of what happens when people lose sight of their core purpose, allow their moral compass to become skewed and operate from a set of values which, in extremis, can endanger the lives of others.

Similar events have taken place in recent years in the financial services industry and the risk outcomes of decisions taken without a solid foundation of moral values has caused untold economic harm to individuals, businesses, governments and nation states.

It is fitting therefore to end this chapter with some words taken from a speech, **The Fairness Challenge**, at the Mansion House on 24th October 2013 by the new Chief Executive of the Financial Conduct Authority, Martin Wheatley.

"So for leaders today – both in business and regulation – the dominant theme of 21st century financial services is fast turning out to be a complicated question of fairness. And at the centre of this debate about fairness is culture and accountability. How do we get firms to do the right thing, whether the regulator is watching or not? How to get senior management to be accountable for doing the right thing?

Is it necessary for the regulator, in a very prescriptive way, to set out what is right, what is fair? The traditional mechanism for dealing with a lapse has been to beef up the rules; to close loopholes in the law as and when they appear; to require more disclosure or compliance with specific processes.

The problem with this approach is twofold. First: it is, 'static'- so it is closing stable doors after horses have bolted. Second: it encourages the very behaviours it seeks to stamp out. In his excellent book ***ethicability®*** *– Roger Steare argues for a more sophisticated interpretation of Integrity in business – one that is not simply defined by the ethics of obedience – what is legally right or wrong – but actually looks towards the ethics of care and the ethics of reason.*

Steare makes the very good point that: 'At their worst, rules, laws, regulations and red tape have a tendency to multiply because they remove our responsibility for deciding what's right'.

His chief criticism? The fact that governments over the years have responded to scandal with rules and regulations, without considering that it was 'the obedience culture' that often failed in the first place.

So today, we are moving back to the future in a sense – with the regulatory system placing far more emphasis on good judgement and less on narrow compliance with a set of rules. Hopefully to a culture where the 'ethic of care' – doing what is right, takes precedent over the 'ethic of obedience' – doing what is allowed."

Extended enterprise risk management is very much about exercising the Ethic of Care as widely as possible with all parties who interact with an organisation. It is about being Care-ful as opposed to Care-less!

Three questions which readers may care to ponder in relation to this chapter are:

- How do you know your people are taking the right decisions?
- Are your values clearly articulated into expected behaviours?
- Are these behaviours measured, monitored and rewarded/penalised?
- Do any claims that you make about your organisational values hold true across your extended enterprise?

The following case studies set out how:

- The multinational diamond and gemstone trading business **De Beers** carefully manages all the risks it faces across many levels and geographies and through complex extended partnerships and relationships.
- The UK retailer and supermarket group J**ohn Lewis/ Waitrose** clearly spells out its ethical stance through its Principles, Responsible Sourcing Programme and Community Outreach, via its two Foundations, so that all its stakeholders are in no doubt as to how they are expected to behave.

The information for both organisations is taken from the exemplary documentation on their respective websites.

References

Hilton A, 2012, Evening Standard – City Comment, London

Heffernan M, 2011, Wilful Blindness, London: Simon & Schuster

Punter A et al, 2011, Roads to Ruin: Airmic

Financial Services Authority, 2011, The Failure of Royal Bank of Scotland, London

Aristotle, c350BC, Nicomachean Ethics – Greece

Steare R, 2013, Ethicability® (5th edition), Sevenoaks UK: Roger Steare Consulting Ltd

Case Study One:
De Beers – building ethics and values across an extended enterprise

"**Best Practice Principles** are more than a set of ethical guidelines. They are an independently monitored framework for all of our business activities and those of our major suppliers and contractors. They ensure that consumers can be confident that international ethical, social and environmental standards have been met in the production of **De Beers** diamonds."

De Beers has made compliance with its Best Practice Principles a legally binding condition of its contracts with Sightholders (see below) and, wherever practicable, with third parties.

Best Practice Principles (BPPs) are a continually evolving standard intended to ensure that consumers buying diamond jewellery can rely on the professional, ethical and technical standards of the gem diamond industry. Supported by an external assurance programme, the BPPs are a mandatory code of ethical business conduct that the Family of Companies, our joint venture partners, contractors and Sightholders all subscribe to.

Sightholders are customers of the Diamond Trading Company who purchase rough diamonds from our mines – have been required to comply with our BPPs since 2005. Contractors that derive 75% or more of their revenue from a De Beers Sightholder or a De Beers entity have participated in the assurance programme since 2008. Contractors that fall below the 75% mark are required to sign a declaration of integrity stating that they are free of any material breaches of the BPP standards.

The BPPs apply to every employee at every level within the Family of Companies and subscribing third parties. As a result, the BPPs cover almost a quarter of a million people, globally, who work in the diamond industry. Employees of the De Beers Family of Companies make up 6% of this number, meaning 94% of those people covered by the BBPs and its assurance programme are employees of Sightholders and their contractors, contractors to the Family of Companies and Diamond Trading Company accredited businesses.

The BPP Assurance Programme is a systematic means of monitoring the compliance of the De Beers Group of Companies, Sightholders, substantial contractors and, where relevant, their business partners in the diamond industry with the BPPs. It has been developed in this new business context to provide evidence to supply chain partners, consumers and other interested stakeholders that the exploration, extraction, sorting, cutting and polishing of diamonds, and the manufacture and sale of Diamond jewellery by entities that are owned or controlled by the De Beers Group of Companies or by Sightholders, are undertaken in a professional, ethical and environmentally friendly and accountable way.

The BPP Assurance Programme comprises a management system and set of assessment tools, a key element of which is Self-Assessment using the BPP Workbook. The information provided by completing the BPP Workbook measures compliance with the BPPs systematically, in accordance with the BPP Requirements.

- All De Beers' companies, Sightholders and contractors that participate in the BPP process must complete and submit annual self-assessment workbooks outlining their conformance with the requirements of the BPPs.
- An independent third party verifier – currently Société Générale de Surveillance (SGS) – undertakes desktop verifications of one-third of total workbooks submitted each year. They also conduct annual onsite verification audits of a sample of all De Beers companies, Sightholders and Diamond Trading Company accredited businesses. In addition our internal audit team assesses all De Beers companies each year.
- When major and minor infringements occur, Corrective Action Plans (CAPs) must be submitted by non-compliant companies. Evidence of corrective action is audited to ensure it is being successfully and continuously implemented.

One of the tangible outputs of the BPP Assurance Programme is an annual report on the business, social and environmental performance of the De Beers Group and Sightholders.

Critically, the BPP Assurance Programme provides a means of checking compliance with requirements relating to anti-money laundering and terrorism financing activities, as well as independent monitoring to ensure that the obligations of the Kimberley Process are satisfied.

The BPP Requirements set out the detailed requirements of the BPPs and incorporate best practice measuring and reporting standards, such as the standard of Social Accountability

International (SA8000) and the Global Reporting Initiative (GRI).

The reporting guidelines and performance indicators of the GRI are used to produce BPP Workbooks, which help to provide assurance to a range of different stakeholder groups.

The BPP Programme Requirements are based on local and international legislation and conventions, including the International Labour Organization (ILO) standards and United Nations conventions, and incorporate best practice measuring and reporting standards such as the Social Accountability International (SA8000) standard and the Global Reporting Initiative (GRI).

Acting in a manner inconsistent with the BBPs can lead to the termination of a Sightholder's or contractor's appointment. A material breach is any serious non-compliance issue that contravenes the core BPPs. Material breaches include but are not limited to:

- The use of child labour or forced labour
- Trade in conflict diamonds
- Non-disclosure of synthetics, treated diamonds or simulants
- Money laundering or the financing of terrorism
- Wilful or negligent acts or omissions resulting in serious injury or death
- Abuse of human rights
- Non-payment of wages
- Causing significant adverse effect to the environment
- Otherwise bringing the diamond industry into disrepute

Source: http://www.debeersgroup.com/en/Sustainability/ethics/Best-practice-principles/

Case Study Two:
the John Lewis Partnership – responsible sourcing through an extended enterprise

"In sourcing our products responsibly, ***we follow robust policies and procedures****, and maintain honest relationships with our suppliers. For many years, we have helped suppliers to build sustainable businesses –* ***commercially, ethically and environmentally*** *– and provide long-term, satisfying employment."*

The John Lewis Partnership's **seven principles** define how they run their business. They are as relevant today as they were when they were set out (in 1929) by the founder, John Spedan Lewis, in the organisation's constitution

Purpose: The Partnership's ultimate purpose is the happiness of all its members, through their worthwhile and satisfying employment in a successful business. Because the Partnership is owned in trust for its members, they share the responsibilities of ownership as well as its rewards profit, knowledge and power.

Power: Power in the Partnership is shared between three governing authorities: the Partnership Council, the Partnership Board and the Chairman.

Profit: The Partnership aims to make sufficient profit from its trading operations to sustain its commercial vitality, to finance its continued development and to distribute a share of those profits each year to its members, and to enable it to undertake other activities consistent with its ultimate purpose.

Members: The Partnership aims to employ people of ability and integrity who are committed to working together and to supporting its Principles. Relationships are based on mutual respect and courtesy, with as much equality between its members as differences of responsibility permit. The Partnership aims to recognise their individual contributions and reward them fairly.

Customers: The Partnership aims to deal honestly with its customers and secure their loyalty and trust by providing outstanding choice, value and service.

Business relationships: The Partnership aims to conduct all its business relationships with integrity and courtesy and to honour scrupulously every business agreement.

The Community: The Partnership aims to obey the spirit as well as the letter of the law and to contribute to the wellbeing of the communities where it operates.

Responsible sourcing

The Responsible Sourcing Code of Practice (PDF size: 50KB) sets out the Partnership's expectations of suppliers. The code is available in 9 languages: English, French, Spanish, Italian, Thai, Turkish, Simplified Chinese, Vietnamese and Afrikaans and can be provided in other languages in request. It is described on the Partnership's website as follows:

"We communicate this code to suppliers and, through our Responsible Sourcing Programme, monitor how suppliers are meeting our expectations and, where problems occur, we work with suppliers to improve labour standards and worker welfare. This is central to our principles and our Constitution and is important to our customers.

All John Lewis and Waitrose own-brand suppliers are required to register on Sedex (the Supplier Ethical Data Exchange: www.sedexglobal.com) - a web-based database to manage ethical and responsible practices within global supply chains. These suppliers must complete relevant self-assessment questionnaires so that we can assess labour standards and working practices at their sites; high-priority sites are also independently audited.

Both John Lewis and Waitrose train Partners on responsible sourcing to support their daily relationships with suppliers.

Our Responsible Sourcing Code of Practice sets out the Partnership's expectations of suppliers. We expect them to be honest about the issues they face and share best practice, so we can work together to make realistic, long term improvements. As we source products from all over the world, we aim to uphold internationally agreed standards of labour. We expect suppliers to treat employees fairly, honestly and with respect for their basic human rights.

All Waitrose and John Lewis own-brand suppliers are asked to commit to meeting the requirements of this Code.

Through our **Responsible Sourcing Programme** we aim to raise awareness of the issues, share best practice and generate feedback so that by working together, we and our suppliers can raise standards in the supply chain.

Raising standards: We appreciate that labour standard issues can occur in many parts of supply chains, and our aim is to encourage suppliers to be honest with us about the issues that they face. We believe in creating long-term partnerships, so we encourage suppliers to make realistic and continuous improvements over time. We have set up various initiatives and tools to help suppliers, including supplier manuals with step-by-step guidance and supplier conferences.

Working with others: We actively work with others to improve our supply chain working conditions. For example, in June 2011 the Partnership joined the Ethical Trading Initiative (www.ethicaltrade.org), which aims to improve the lives of workers internationally through an alliance of companies, trade unions and voluntary organisations. The ETI focuses on workers across the globe that make or grow consumer goods. It builds alliances in key sourcing countries and internationally, to address problems that occur not only in individual workplaces, but also affect entire countries and industries.

Trading fairly

We care about trading fairly with our suppliers and contributing to the sustainable development of the communities where workers live.

In keeping with our principles of fairness, flexibility and openness we have taken constructive steps to help the businesses we trade with, especially small enterprises, to remain viable. For example:

- We give suppliers clear guidance on payment terms and pay them on time. This is reflected in the Partnership becoming a co-supporter of the voluntary scheme: Government's Prompt Payment Code.
- Through Waitrose's milk price pledge, we agree to pay our dairy farmers a premium over the market price. Our pricing model for British pig farmers, takes into account the cost of sustainable production methods, ensuring our suppliers receive a fair return.
- Since February 2010, Waitrose, along with all major food retailers, is required to comply with the Groceries Supply Code of Practice (GSCOP). GSCOP, the result of the Competition Commission's investigation, protects suppliers from excessive risks and undue costs. A Waitrose project team ensures compliance and the GSCOP terms are communicated to all suppliers.
- One of our models for community engagement with our suppliers is the **John Lewis Foundation**, established in 2007 to improve the wellbeing of our suppliers' communities, in the UK and overseas. The Foundation makes grants to improve disadvantaged communities in which suppliers live and work.

The Waitrose Foundation is a supply chain partnership that returns a percentage of profits from the sale of produce to fund projects chosen by the farmers and smallholders who grew it. Launched in South Africa in 2005, Waitrose believes the Foundation is a model for the future of socially responsible trading.

- By putting some of our profits back through the supply chain, farm workers are able to invest in their own communities, and in turn deliver the best quality products for our customers. Locally-elected worker committees decide what the community needs most, such as crèches, adult education classes, and recreational facilities projects to improve health standards. In 2008, we introduced tertiary education bursaries. Our first two students graduated in financial management from Stellenbosch College in 2010 and the scheme is now funding the studies of seven more bursary students.
- In South Africa, the Foundation also links in with the South African government's strategy of Black Economic Empowerment. This is a framework intended to support the participation of black South Africans as owners, managers, professionals and skilled employees in the agricultural sector."

Sources:

http://www.johnlewispartnership.co.uk/csr/our-approach.html

http://www.johnlewispartnership.co.uk/csr/our-products-and-suppliers/responsible-sourcing.html

Chapter 7: Risk, innovation and the extended enterprise

Dr Keith Smith FIRM

The importance of innovation

In organisations, whether for profit or not, wilful neglect of innovation is widely recognised as a risky strategy. Within an extended enterprise that innovation may come from within your supply rather than from within your own organisation. In this chapter, we will look at innovation in the supply chain and more explicitly, innovation as it applies to extended enterprises. Before reading this chapter, read or at least review chapter 1 which gives an overview on complexity in organisations and chapter 6 on 'Building Trust'.

Why innovate?

Reviewing the extinction timeline in Figure 7.1 you see some of the popular products and services that have given way to newer alternatives. You may be surprised by how many you have forgotten. Consider for example 'film processing' shown in above graphic. Film processing has largely given way to digital cameras and the viewing of images on digital devices. (See also the IRM risk Culture guide for the Kodak case study). Chemical based film processing was a widespread and profitable industry, but its fall from popularity was still relatively quick. Neither scale nor brand power was enough to defend against the consumer benefits associated with the innovation of high quality digital imaging.

Shorthand is a service example, a skill in widespread use before the advent of the word processor. Without the benefit of hindsight, who would have made the link between the innovation of the word processor and the demise of shorthand? Even more difficult to see was the demise of the office typist role, as people changed the way they worked with the innovation of word processing. Innovation does not just replace old products with new ones, innovation is behind all the sea changes in society affecting the way we work, the services we expect and the skills we value as a society.

While innovation is a source of advantage and a necessity for ongoing survival, it is also a source of substantial risk and uncertainty. How organisations approach the issue of innovation is full of important choices and the risks associated with each choice should be carefully evaluated.

Staying ahead in a chosen market by being the leading innovative organisation in a sector is one approach, but that can be a costly high risk strategy. The alternative of adopting or acquiring the innovations of others may work equally as well and in some cases may be a better long term strategy.

This chapter provides guidance on how and where to look for many of the uncertainties associated with innovation in complex organisations. The chapter also touches on some of the steps needed to protect an organisation from having its innovation activities compromised. It is not an exhaustive guide, but rather a primer aimed at helping risk practitioners get started with this complex area of risk management.

Innovation as a strategic choice

McKinsey have carried out research into what makes a company successful in innovation[6]. Through that work they dispel the myth that all you need is some fun filled toys, housed in a brightly coloured break out room to spawn innovation. McKinsey found that successful organisations aligned their innovative effort towards clear goals through a practical working definition of what innovation meant for them as an organisation. The academic classifications of incremental, breakthrough, etc. appears to be largely irrelevant in achieving success and this particular classification approach is not used in this chapter.

McKinsey also found it was important to protect innovative investment at the Board level. Management also had to accept that the range of uncertainty associated with innovation risks may be higher than in normal day-day business. Obvious, perhaps, but saying and living these commitments are not the same thing. In some cases, maybe a different legal entity is required to free the innovation element from organisation controls that may apply in an established organisation.

Some of the uncertainty with innovation stems from the activity of development itself, but some is a result of the lack of familiarity the organisation will have with

6. This research was discussed in an interview given to Boardmember.com by Maria Capozzi, an innovation expert with McKinsey and Co, on 21st February 2013

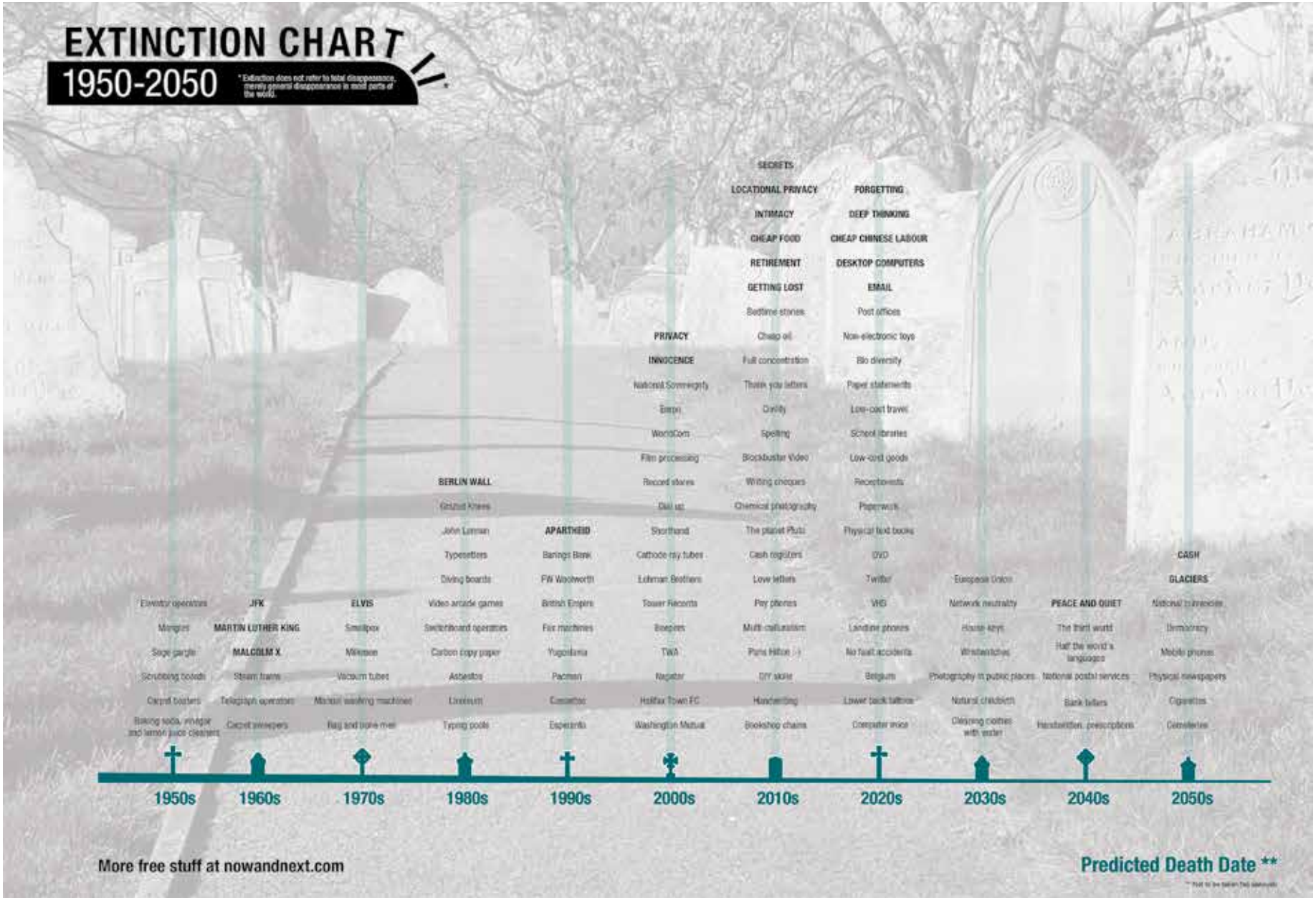


Figure7.1: Extinction Chart. Reproduced with kind permission from www.nowandnext.com

the innovative areas in which they are trying to work. Overconfidence may be a problem fuelled by familiarity with the current market rather than familiarity with the true innovative needs driving towards the future market.

Key questions to ask at an early stage in the cycle of innovative development are:

- Is there clarity in the strategic role innovation plays in meeting the organisations objectives?
- Is the definition of innovation used within the organisation grounded in useful practical outcomes aligned to the organisations goals?
- Is the innovation team appropriately resourced and protected within the organisation's management framework?
- Do you have access to the skills you need and if not, how will you acquire access to those skills?
- Is the risk Appetite for innovation articulated and understood within the whole organisation?
- Do you need to form a different organisation with a structure that can support the risks you need to take?
- Are the financial and non-financial resources available to support innovation projects?

There is no intention to condemn 'blue sky research' if the goals of the organisation include that kind of investigative research. Indeed, there are organisations for which this kind of research is in the majority of innovative effort being carried out. Nevertheless, even in this category, organisations without a clear, well-articulated strategic direction are considered as running a risk of underperforming.

It is worth remembering there are many ways for an organisation to acquire access to innovative skills. Understanding the different models for bringing innovation into an organisation and the complexity behind some of them is key. Guidance on this is provided later in this chapter.

Lack of innovation as a risk

Given the importance of innovation, a lack of innovation, particularly around the core products and services of an organisation, should be considered a serious threat. Every Board should ask itself the following questions:

- Is appropriate innovation being considered seriously in all areas of the organisation?
- Is the organisation prepared to take enough risk to foster appropriate innovation?

(This second question is an issue of risk Appetite and the IRM guidance on risk Appetite and Tolerance is recommended reading for this subject.)

A framework to explore the external threats and opportunities can be a useful tool to ensure a comprehensive review of competitive forces that may drive the need for fresh innovation. A potentially useful framework, at least for a macro-economic view is Porter's Five Forces model (Porter, 1980)

Figure 7.2 Porter's Five Forces model

This model is used by systematically considering the effect and out turn resulting from each of these identified market drivers. For example: in a market where there is significant oversupply, buyers may be seen as empowered and able to drive hard bargains. This will result in a different risk profile from a supplier driven market, where buyers may need to pay a premium to get what they need.

Innovation risks are often associated with the threat of substitutes and the entrance of new players. Substitutes can be more difficult to spot as they change the market they are serving. For many years, horses provided transport and power which met the needs of society at that time. Their use was prolific and there was substantial supporting infrastructure with both stabling and shoeing services available in every small town. With the development of the internal combustion engine, the horse was soon displaced as the main source of power

within society. This innovation did not just affect the trade in horses, but created widespread changes in society and substantially increased our flexibility to travel.

Porter's model has been suggested as an option for a macro economic view, as more recent work (Grundy, 2006) suggests that at the micro economic level, many other factors may be behind the need to innovate. For example, quality of service, market attractiveness and even emotional factors such as tradition may have considerable influence on the scope of innovative thinking.

Innovation timeline

The Eureka moment of innovation may well be an overstated occurrence. Consider the development of the World Wide Web which is regularly held up as one of the great innovations of the modern age. The process started with the connection and transfer of files between two computers in a point to point connection. That led to more sophisticated connections with built in redundancy and signalling to route signals between multiple computers. Lines were found to be noisy and error correction was included to address the loss of data. With further development and the concept of layered signalling models, the application running on the computer became somewhat detached from the data stream that supported it. With a bedrock of data exchange, electronic mail was possible and this was followed by a protocol that supported browsers from scientists and engineers at CERN in Switzerland. This whole process has already had a life history of some 35 years and it's not over yet. Consider how the risk profile changed at every stage of this progressive innovation of the web. Initially, the risks were technical rather than commercial. Now, the loss of data is an economic risk for many organisations and the technical connections themselves are just low value commodity services.

Innovation clockspeed

Charles Fine, an MIT professor, looked at the cyclic nature of industry for its value in developing Competitive Advantage (Fine, 1998). He makes several points in this book, but there are two that are worth highlighting for this chapter. Fine argues competitive advantage is a transitory position and if not renewed, competitive advantage will be lost to a competitor at some stage. Taking this a step further Fine also identified that some industries introduce new products at a faster rate than others. A suitable comparison would be between digital cameras, new versions of which are released within months of each other and white goods that may be on the market, almost unchanged for a number of years. He labelled this cyclic time orientated development "Clockspeed" and suggested that the slower clockspeed industries can learn from the faster ones. This approach leads to several questions related to innovation that every organisation should ask itself:

- Do you have competitive advantage and are you doing enough to renew it at a frequency that compares to the market norm?
- Who is capable of taking your competitive advantage from you? Bearing in mind that competitor may be a new entrant in the market with a substitute product or service.
- Is there a faster industrial clockspeed sector to study which is useful for you to learn from?

Before we leave the subject of clockspeed, Charles Fine's book was the inspiration behind risk Clockspeed (Smith & Borodzicz, 2008) which looks at risk from the perspective of management information availability. This is also relevant as in innovation, many of the risks will fall into the fast risk Clockspeed category and as such will require a different style of management to many other risks an organisation may face. When assessing the risks associated with innovation looking at their risk Clockspeed is highly recommended to make sure the right management style is being used to address the risks.

Technology risk assessment

When engaging with innovation it is easy to get caught by expanding budgets and constantly moving milestones. One strategy for helping to manage this risk is to assess how much and how risky the innovation content of a product or service is using a Technical Readiness Index (TRI).

Several TRI schemes exist, but it may be appropriate to design one specific for an organisation based on what the organisation does. The basic principle is to assess the degree and viability of the innovation required and assign a risk level to that assessment using a scale. For example, innovating a new elastic band based on current material technology, where the new version has a unique colour, length and tension (given by the materials cross section) would score low on TRI. The technology is largely known, research will be limited and experience from designing other elastic bands is available to quantify the R&D time. On the other hand, the O ring on the US space shuttle, which is just a band of elasticated material, was clearly much higher on the TRI scale. With this O ring the range of temperatures and pressures faced pushed the boundaries of this type of elasticated seal technology to its limit. New materials,

new test methods and new assembly methods were all required. The design and later redesign of the O ring that failed on Challenger was expensive and time consuming in every way (Dalal, Fowlkes, & Hoadley, 1989). While popular with military equipment providers, the TRI approach does not ensure that programmes will not get out of hand and the example of the Joint Strike Fighter development (Sullivan, 2013) – see box below - illustrates how innovation can still run away with budgets and time.

Case study:

the US Government Report on the Joint Strike Fighter Development (M. Sullivan. GAO. June 2013)

The new total acquisition cost for the JSF is $395.7 Billion, up $117.2 Billion from the 2007 baseline. In 2011 only 6 of the 11 important objectives was met. Only 21% of the flight testing is complete with the most challenging tasks still ahead.

Quote. "Developing and integrating the 24 million lines of software code continues to be of concern".

Quote. "Most of the instability in the program has been and continues to be the result of highly concurrent development, testing and production activities"

Protecting innovation

Failing to protect innovation can cost an organisation its future, but protecting innovation can be costly too. Protecting innovation is a specialist area covering international design, patent and copyright protection, all of which have legally enforceable rights. Many of the laws that apply to products and service protection are backed by international agreements and this network of agreements adds to the complexity of this issue. Given the complexity, specialist advice is highly recommended. As for the associated risks, these will be driven by the scale of losses or unrealisable opportunity if adequate protection is not in place.

Innovation and the extended enterprise

The extended enterprise was more of an issue of recognition for the way organisations had evolved to work together rather than a new discovery as the issue was never hidden. Organisations had already formed extended enterprises before Chrysler's CEO formally used the term in the early 1990s (Boardman & Clegg, 2001).

Following recognition of the extended enterprise as a commercial architecture, research was undertaken to understand the forces and tensions that exist within members and the effect organisational boundaries may have. Many of the issues found to be critical in an extended enterprise were exaggerations and variations of issues that arise in any large organisation. For this reason, many of the risk considerations raised in this chapter apply equally to any large organisations as well as extended enterprises.

Risk in open innovation

Open innovation is a particular form of extended enterprise which is proving to be increasingly popular (Van de Vrande, De Jong, Vanhaverbeke, & De Rochemont, 2009). The concept is that organisations do not need to place such tight control over things like idea generation, product and service testing or even design. By opening up their innovation and development structures by publishing information they have so far, anyone can freely contribute. A good example of this is the Beta testing of software, where companies such as Microsoft launch Beta products under special licence so that people may use and improve the product. Open Source is also a form of open innovation.

From a risk perspective, open innovation is not risk free. Publishers need to be confident that they are not giving away excessive amounts of their intellectual property or providing the information competitors need to counter any market advantage that may be realised. Here are some questions to ask about open innovation to surface the risks that may be involved. See also the issue of Integrity risk:

- Is open innovation the best way to get the competitive advantage you are seeking with this innovation?
- Are you placing the right amount of information into the public domain to get the innovation you seek?
- Are you placing information into the public domain that your competitors may be able to use against you and if so, will the benefit outweigh the losses? (The value question)
- Do you own or have rights to all the information you are placing into the public domain?
- Do you have the right processes in place to capture and capitalise on the fruits of this innovation? (Value realisation)

Frugal innovation

Considered a relatively new but none the less a growing concept is 'Frugal Innovation'. This type of innovation is aimed at reducing the cost of a product by carefully selecting the features and requirements necessary to address an identified market. This approach to innovation does not produce lower quality goods, so much as highly specialised ones fit for markets that have previously been overlooked. With such a definition, it is easy to see some of the additional risks associated with this kind of innovation. Again, the list is not meant to be exhaustive, but is intended to promote deeper consideration of the issues:

- Has the market been well researched and are the product requirements fully understood? (This is important in any innovation, but essential in a frugal innovation as over specification is a particularly undesirable outcome)
- Is there a profitable balance between the innovation costs and price point available in the target market?
- Given competition between similar products, where one is provided at a reduced specification, is the differential in price point sustainable to support multiple markets?
- Is the life expectancy of the frugal product viable?
- Have the innovation costs truly been minimised or is innovation required in other areas such as component sourcing or assembly to meet the best market price point?

Risk when clustering

One successful approach to foster innovation in an extended enterprise came with clusters (Mudambi & Swift). If a number of high energy innovative collaborative enterprises are co-located and collectively they have the capability to deliver a product or service, then the co-location helps. This concept has been taken up strongly in the Middle East within the Emirates of Dubai and Abu Dhabi. Cities have been created to foster shared innovation in areas such as media, sport, finance and communications.

Here are some questions to help surface the risks associated with clustering:

- How close is your organisation both geographically and relationship wise to potential sources of innovative input? Do you need to relocate?
- In clustering with these organisations, are you with the right group?
- If your relationship changes with each organisation in this cluster, will you still be in the right place for your business?
- Are you adequately engaged with the local cluster to reap the benefits of your location?

Communication risks

Back in the 1990's a research project into the extended enterprise called PIPSEE (De Montford University) concluded that inter organisation communications was a real problem for the extended enterprise. Terminology was an issue, but also information paths. In some cases, the formal recognised information path was not the source of information that partners relied upon. With Information Security being a priority, information sharing for the purposes of innovation is an area of risk that must be evaluated carefully as often there are competing challenges. Here are some questions to explore the risks involved:

- Are appropriate channels of communication with your innovation partners in place?
- Are you at risk of informal information exchange channels emerging through the growth of personal relationships between staff?
- Is the audit of information sharing and information security appropriate for the value of the information being shared?
- Are there adequate safeguards in place on IT systems shared with your partners?
- Are there adequate processes in place to manage the natural churn of people and organisations who may be involved in your innovation relationships?

Integrity risk

When the extended enterprise is innovating software, the trust relationship is inevitably high as it may be difficult to fully test what is delivered. Integrated software integrity may be compromised by third party modules of software built into a larger program. When software is involved, the following questions may be relevant to surface any additional risks.

- Are you relying on third party software to maintain the integrity of your innovation?
- If the integrity of your innovation is compromised by a third party supplied module, what are the likely consequences and are you adequately protected?

- Are you confident with the processes and procedures your innovative partners have in place to ensure the integrity of the software they are providing?
- Are you confident about your acceptance test process?
- If you are going to use open innovation, can you be confident about the content and quality of contributions?

Five models of innovation

The process of innovation has itself been subject to innovation and there are various models to describe the different forms of innovation organisations engage in. Rothwell (Rothwell, 1992) articulated five models that he arranged as generations indicating that the models used have become more sophisticated over time. Rothwell's descriptions are listed as follows and a useful critique of these can be found in a paper by Hobday (Hobday, 2005). In reality, there are probably examples of innovation based on each of these models still in existence today and these timeframes should be considered as loose guides at best. Indeed, it could be argued that SMS messaging on mobile phones (circa 1991) was an example of successful technology push; as the market pull at the time did not reflect the high demand for messaging that rapidly developed when the service became available (Xu, Teo, & Wang, 2003).

The value in the five models from the risk point of view is that collectively they provide a useful set of labels for identifying the innovation processes at work in any relationship. These labels can also be associated with specific areas and types of risk:

- Which of these models are in use within the organisation under review?

GENERATION	ASSOCIATED DATE RANGE	EXPLANATION AND KEY RISKS
1: Technology Push	1950s to mid 60s	Simple linear process. Emphasis on R&D to develop new products for the market. **Risks associated with developing products and services that the market then rejects**
2: Market Pull	1960s – 1970s	Market demand pulls new products and services through a linear process. R&D reactive to market demand. **Risks of underperforming products and services where the market players did not see a useful innovation that competitors then incorporate. Market pull may also lead to products and services with short lifetimes as markets tend to deliver short term expectations**
3: Coupling models	Mid 1970s – 1980s	Sequential model with feedback loops. Typified by interaction between Marketing and R&D to balance product innovation with market need. **Risk of delay to market and confusion where product or service is always subject to change. As with simple market pull, there are also still risks associated with lack of comprehensive innovation and short term views**.
4: Integrated model	1980s – 1990	Parallel development with integrated teams. Aim to make innovative product that was cost effective to manufacture. Introduction of joint ventures and partnerships to combine strengths. **Risk that locked in partners are mismatched or the network formed is too weak to compete against competitive networks. However there is a lot of opportunity in this model to integrate leading suppliers to give world beating products and services through an established pipeline of expertise**
5: Systems integration and networking	Post 1990	High integration, parallel development. Collaborative research. Emphasis on flexibility and speed. **Threats exist around information sharing, security and collaboration. Research has shown that informal information transfer paths become established . On the other hand, opportunities to be very creative can also exist and many high tech products rely heavily on this model**

- Are these models appropriate?
- What risks are faced as a result of the innovation model that is in place?

Modelling the organisation

To systematically assess the risks associated with the innovation processes in any organisation, it is necessary to understand the flow of innovative activity around organisation. It is also important that every part of the organisation is considered, as innovation is not limited to the core activities the organisation offers. Innovation can occur in any part of the organisation and at many levels of depth.

A detailed set of process models for the organisation will of course be one way to map the organisation for this purpose, but such a full set is unlikely to exist in any simple form. For the purposes of risk management, the value contributed by the innovation process is perhaps easier and more interesting, where value can be seen in terms of achieving the organisation's objectives.

Michael Porter, the Harvard Business School Professor, introduced the Value Chain concept in his work on competitive advantage (Porter & Millar, 1985) and with that concept he introduced the view of an organisation as shown in Figure 7.3 below.

The Value Chain is not perfect for our specific risk use as it was not necessarily aimed at innovation risk identification. In addition the Value Chain is not the only valid view of the organisation that could be used, so the intention here is just to provide a least one valid option for understanding innovation within any organisation.

This method of modelling the organisation has imperfections considering the risk management purpose being addressed, but it does have the following useful characteristics:

(1) The Value Chain model may be used for both 'for profit' and 'not for profit' organisations where the value and margin are seen in terms of non-financial gains

(2) The focus on value generation is useful in terms of assessing the impact any risk may have on the organisation's objectives

(3) The model can be applied to all types of organisation, so in a complex group of organisations, the model can provide consistency across the group

(4) In an extended enterprise, the risks associated with key suppliers and other stakeholders can also be mapped out in terms of their Value Chain. Applied

Figure 7.3: An illustration of Michael Porter's value chain

recursively, the model may be used to analyse the whole extended enterprise and so surface any hidden conflicts and misaligned goals

(5) It is exhaustive in that all parts of any organisation can be incorporated within the headings used in the model

(6) The model allows for innovation in any part of the organisation

Given the 'innovation risk' use being made of the Value Chain, there are some enhancements that could highlight other considerations that matter in the management of risk. An alternative value model is shown in Figure 7.4 below which can be distinguished in type by referring to it as the risk Based Value Model of the organisation. Again, the model chosen should be right for the practitioner and for the organisation and this is presented as no more than a candidate in that choice

(For each of these two models (Value Chain or risk Based Value Model) consider the innovation being carried out in each area of the business. Consider the risks arising from the innovative process employed, the information shared, the trust that exists and the IPR generated. Consider too the effect delays in information sharing, the mismatch of language and the multiple sources of feedback that exist. Consider also the external environment and how that may directly or indirectly affect the behaviours of partners?)

This rendition of the Value Model has additional features over the standard Value Chain representation:

(1) The final end 'margin' element has been removed and the 'Value' concept is considered to be the value generated by each part. This allows tight coupling between the innovations taking place in any part of the organisation to the value it brings to the organisation

(2 The inferred left to right flow has been removed as this isn't helpful for identifying risk in the innovation processes and may lead to some incorrect assumptions about timing

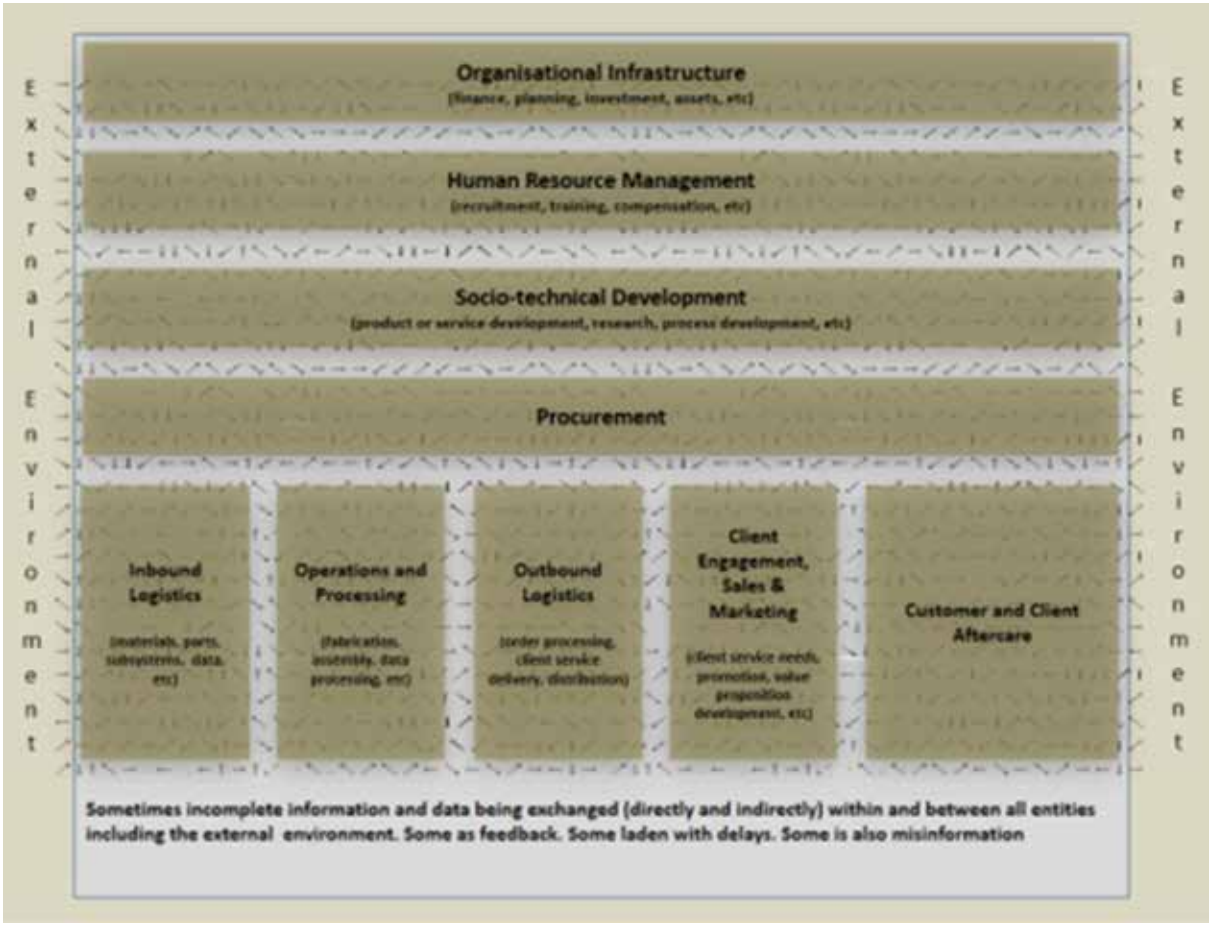


Figure 7.4: The risk Based Value Model of an Organisation

(3) This risk Based Value Model aligns with the systems view of risk as covered in other chapters of this document

(4) The complex flow of information is represented by the arrows recognising that risk may be a feature of communications, particularly in an extended enterprise. The model also includes the important consideration of delays and feedback that exist in a real enterprise and which may be a source of additional risk

(5) The model has been set in the wider context of the external environment where changes could affect the innovation processes and the value generated within the organisation.

Value assessment

The determination and distribution of value is an important part of this chapter on risk and innovation. For a product it is relatively easy to disaggregate the product into its component parts and assign both cost and added value to the parts. Portelligent Inc carried out such an exercise on the 5th generation IPod that was sold in late 2005. This Portelligent work was then revisited in 2007 by a team at the University of California (Kraemer, Dedrick, Linden, & Center, 2007)

Apple acted as an integrator of these parts so this is an extended enterprise view of the IPod with each of these parts being supplied by a number of suppliers to Apple. The purpose of this illustration is to show how the value may be tracked and how not every partner extracts equivalent value. Given the actions of partners will be determined by the overall worth in participation such a view may help determine where some of the co-operative risks may lie, particularly if the impact of participation on the partner is substantial.

With a service, particularly if the service is provided in a not for profit organisation, the disaggregation and assigning of value through the complexity of players may be more difficult to do and the concept of value may not be measured in direct financial terms. However the usefulness of such an exercise may justify the effort, even if the figures produced are just good estimates.

In some relationships the value of participating in an extended enterprise may not be for any direct monetary outcome. The value of participation may be to raise profile, positioning of the organisation or in a not for profit relationship, participation may be based wholly on a social gain value model. Indeed, the value of participating may be based on a mixture of rewards, as value is a quality assigned by the recipient. However

COMPONENT	ESTIMATED FACTORY PRICE	ESTIMATED GROSS PROFIT RATE
Hard Drive	$73.39	26.5%
Display Module	$20.39	28.7%
Media processor	$8.36	52.5%
CPU	$4.94	44.8%
Assembly and Test	$3.70	3%
Battery	$2.89	unknown
Display driver	$2.88	24%
32GB memory	$2.37	28.2%
Back enclosure	$2.30	26.5%
PCB	$1.90	28.7%
All other parts	$21.28	unknown

Table 7.5: Summary of parts from Table 1 in 'Who Captures Value in a Global Innovation System?' PCIC 2007

value is determined, the principle here remains the same, for the evaluation of risk, it is important to understand the value each party derives from their participation.

Relationships

Another perspective to take when assessing the risks associated with innovation is the relationship held with other parties engaged in the innovative process. This section simply aims to suggest some lines of enquiry under the heading of Relationships.

- Who is involved on a day-day basis with the process of innovation?
  Risks may be associated with these personal relationships and the commitment individuals have to each other.
- What is the legal relationship between the parties involved in the innovation?
  For risks around future legal challenges based on the relationship structure.
- Are IPR ownership issues clear? Innovation may not result in formal IPR being registered, but almost certainly innovation will lead to increased value being generated for one or more parties. Any lack of clarity around IPR issues needs to be considered as a risk.
- How is the value distributed?
  If there is an imbalance in the way the value created by innovation is shared, then there is a risk that irrespective of the formal legal relationship, one or more of the parties involved may seek to rebalance the equation.
- Are there misaligned goals?
  Frequently overlooked, it is useful to consider the goals held by each party involved in the innovation. It is wrong to assume they are the same, particularly in an extended enterprise. Misalignment of goals may yield a number of surprises, most of which are likely to be unwelcome.
- What is the balance of power?
  Again, something that is frequently overlooked, but an issue that was widely researched as part of the extended enterprise work in the 1990s. A large integrator organisation may exercise considerable power over a smaller supplier. This may force the supplier to act defensively, or be a barrier to that supplier in terms of sharing their innovative skills. At the other end of the spectrum, being dependent on a large supplier, for whom the organisation is just a small customer, is a dangerous place to be. Power balances are at the heart of the Five Forces model and this relationship issue is why its use is recommended (The Kitty Litter case study found later in this chapter is an example of this form of risk).
- How is terminology used?
  Communications is a common source of risk in any situation. Research into the extended enterprise (See the footnote on PIPSEE) found that terminology mismatch between organisations with a different language heritage can be a particular problem. More to the point, this same research project found that such mismatches can be persistent over time.
- How is influence exercised?
  While a relationship may suggest influence, the exact nature of that influence and the effectiveness of influence may need to be considered. Personal and entity level relationships need to be considered.
- What is the level of trust?
  Trust is covered more extensively in other chapters of this guide. It is raised here in the context of innovation as a particularly acute consideration as without trust, innovation between parties is unlikely to happen.

Regulation and society

Strange as it may seem, both regulation and society pressures may be substantial drivers in innovative practice. In children's care for example, the tragic cases of 'baby P' and Victoria Climbié[7] both proved to be strong forces for change and innovation in child care practices. In the field of commerce, the Solvency II regulations are currently driving innovation in the insurance market.

The impact of regulation and society is not always targeted at the organisation or sector in any direct way. Changes in Government and Governmental policy such as taxation can be a consideration when investment in innovation is being considered

Within the risk Based Value Model, the addition of the external environment includes the innovative forces of regulation and society. However this is one area not covered by Porter's Five Forces model which is illustrative of why consideration should be given to applying a range of techniques in any risk analysis.

7. Both of these cases involved the tragic long term abuse and final death of young children. Societal outrage led to inquiries and legislative changes to try and prevent such events ever happening again.

For all organisations, the 'green agenda' and the 'social responsibility agendas' are specific cases that should be assessed as part of the innovation risk universe. It may be useful to consider the following levels of Corporate and Social Responsibility (CSR) as part of a review of innovation risk. Unlike most of the above where the dominant issue has been threats, this is an area where the opportunity side of risk management can be a significant consideration.

Again, based on work by Michael Porter (Porter & Kramer, 2011) who has contributed a lot to strategy and competition, consider these three levels of CSR.

1: Philanthropy. No innovative interaction, no new value being generated, but gifting of some profit to good causes.

2: CSR. Gifting of funds and adherence to social expectations such as fair trade, social responsibility towards workers (for example no child labour) and open reporting of CSR activities. No direct innovation results and no new value generated, but innovation may be required to maintain socially accepted levels of CSR as expectations change.

3: Creating Shared Value (CSV). Interaction with smaller suppliers and even sole traders to increase the value generated in the value chain for later distribution. For example, a large agricultural organisation may work with local farmers to improve practice, reduce costs and increase yield. The essential difference in CSV being that new value is created by this more interactive level of working.

On first reading, the significance and value of applying these levels to any analysis of the risks associated with innovation may seem obscure. However, any interaction with external organisations, societal units or even individuals may carry some threat or be an unrealised opportunity.

For example; philanthropic giving may be a missed opportunity if the money given may be used as part of a programme of shared information and innovation. CSR based giving may be more targeted and the value distributed is shared within the industry, but again is there missed opportunity to use the funds to generate new value (the CSV model)? Or, are the CSR activities providing funds for unseen innovation in the supply base that may be exploited and the risk is that the organisations CSR structure is hiding this?

When engaging with Creating Shared Value (CSV) organisations still need to consider and address the associated risks. Is there clarity in who will own the IPR? Is there reasonable sharing of value, or is the organisation exposed to claims of exploitation? Perhaps these issues can be easily resolved as part of the engagement contract, but where a large organisation is working with poorly educated groups in poor countries, the risks of unintended consequence are higher.

Case study:

Kitty Litter

(The following may be found in Clockspeed by Charles Fine. Perseus Books. 1998. P106)

For Chrysler, the Grand Cherokee Jeep was a profitable model. Chrysler mapped its supply chain and found that important castings for the engine were ultimately dependent on a small niche supplier of casting clay ceramics. The problem was this supplier had been managed down to such an unprofitable position by the power of the chain above them that they were forced to think of new markets to address. Without informing the rest of the supply chain, the decision had been made to exit the casting market and exploit a different property of their ceramic technology - the ability to soak up cat urine for the kitty litter market. Such a move by this small supplier would have spelt disaster for Chrysler had they not found out in time.

This little anecdote highlights the risks that can arise from power imbalances and inappropriate contract terms when dealing with smaller, weaker suppliers

Contracts and risk sharing

While an organisation sat within a healthy extended enterprise may benefit from key supplier expertise, the key supplier also benefits from the relationship and this raises the opportunity of risk sharing. On the one hand, natural justice suggests any party who benefits in the relationship must bear some responsibility for the pool of risks that arise. On the other hand, the size, economic power and access to resources for the participants are frequently quite different. The point to bear in mind of course is that all the participants in an extended enterprise based innovation venture are key. In formulating contracts for innovation, one of the biggest risks is in the over use of positional power to create or even impose a risk sharing agreement that off loads risk in an inappropriate way. This is an extension of the 'Kitty Litter' problem (see case study below) in which power imbalance is the real issue.

When entering in a Creating Shared Value relationship, the power and resource imbalance may be even more pronounced than in an extended enterprise where the partners are likely to already be involved in a tight commercial relationship. It is quite possible that one or more of the Shared Value participants could be considered as commercially or contractually naïve when compared to some of the larger more established organisations.

When an innovative or CSV relationship exists, there is a risk that it is seen as being outside the normal day to day business of the organisation. This in turn may lead the organisations concerned to exclude the venture from its process of audit (See Audit elsewhere in this document). This may be a significant omission as the role of innovation plays an important part in the future of all organisations. Audit, particularly shared audit, may also help ensure that each party is dealt with fairly and this is a key ingredient for the trust relationship on which success is dependent.

In an extended enterprise or CSV relationship, whether related to innovation or not, there is always the prospect of unintentional risk sharing. That is to say one party may be exposed to a risk that is caused by the acts or omissions of another party. For clarity and to emphasis the different nature of this unintentional risk sharing we could use the term 'inherited risk', where the inheritance could come as a surprise to one or more of the participating organisations. In an extended enterprise or CSV relationship there are several reasons why inherited risk may not come to light. Consider the following as example reasons why inherited risk needs due consideration:

- A partner may hide a risk that affects another partner out of concern that the risk may jeopardise the relationship
- A partner may be insufficiently risk aware to uncover the risk in the first place. This is a problem that may be exacerbated by size and resource issues
- A partner may assume that the other partner is aware of the risk and accepts the consequences as an aspect of the business they are in

  The following questions are provided as a primer for some of the risks that may arise from the contractual and risk sharing arrangements that may exist for innovation and CSV relationships:
- How equal (power, resources size, etc.) are the partners and is there evidence that any imbalance is leading to inappropriate risk sharing?
- Can any of the participants be considered as disadvantaged through contractual or commercial awareness such that this may cause a contractual relationship imbalance?
- Is the risk sharing clear and are all parties involved able to manage the risks they have?
- Is the contract fair in the way it manages risk and continued areas of uncertainty that may arise?
- Is the contract adaptable such that unanticipated situations can also be raised and managed in a fair way?
- Are there any risks that were previously hidden and what were the reasons behind these risks being hidden in the first place?
- Is there sufficient trust between the parties for risks to be declared without the fear of retribution or blame?
- Are there any inherited risks that transcend the boundaries between organisations?

This chapter has been written to provoke thought and to open up a list of potential issues. It should not be considered as an exhaustive list of issues to be considered nor would every issue apply in all circumstances. As in all matters of risk, there is no substitute for expertise.

In conclusion the Board and risk practitioner should be comfortable they can answer the following:

1. How dependent is the organisation on innovation in the supply chain and is that in balance with innovation taking place within the organisation?
2. Are all parts of the organisation willing to innovate and change to suit changing market demands?
3. Are there any areas where the propensity to control (see IRM on Risk Appetite) is stifling innovation within the organisation?

References

Boardman, J. T., & Clegg, B. T. (2001). Structured engagement in the extended enterprise. *International Journal of Operations & Production Management*, 21(5/6), 795-811.

Dalal, S. R., Fowlkes, E. B., & Hoadley, B. (1989). risk analysis of the space shuttle: pre-Challenger prediction of failure. *Journal of the American Statistical Association*, 84(408), 945-957.

Fine, C. H. (1998). *Clockspeed Winning Industry Control in the Age of Temporary Advantage*. Reading, Massachusetts: Perseus Books.

Grundy, T. (2006). Rethinking and reinventing Michael Porter's five forces model. *Strategic Change*, 15(5), 213-229.

Hobday, M. (2005). Firm-level innovation models: perspectives on research in developed and developing countries. *Technology Analysis & Strategic Management*, 17(2), 121-146.

Kraemer, K. L., Dedrick, J., Linden, G., & Center, P. C. I. (2007). Capturing Value in a Global Innovation Network: Comparing the iPod and Notebook PCs. Unpublished Presentation by University of California PCI Center.

Mudambi, R., & Swift, T. Multinational enterprises and the geographical clustering of innovation. *Industry and Innovation*, 19(1), 1-21.

Porter, M. E. (1980). Competitive strategies. *New York*.

Porter, M. E., & Kramer, M. R. (2011). The big idea: creating shared value. *Harvard Business Review*, 89(1), 2.

Porter, M. E., & Millar, V. E. (1985). How information gives you competitive advantage: Harvard Business Review, Reprint Service.

Rothwell, R. (1992). Successful industrial innovation critical factors for the 1990s. *R&D Management*, 22(3), 221-240.

Smith, & Borodzicz. (2008). risk Clockspeed: A New Lens For Critical Incident Management. *Systemist*, 30(2), 354-371.

Sullivan, M. J. (2013). F-35 *Joint Strike Fighter* (No. GAO-13-690T). Washington: GAO.

Van de Vrande, V., De Jong, J. P. J., Vanhaverbeke, W., & De Rochemont, M. (2009). Open innovation in SMEs: Trends, motives and management challenges. *Technovation*, 29(6), 423-437.

Xu, H., Teo, H. H., & Wang, H. (2003). *Foundations of SMS commerce success: lessons from SMS messaging and co-opetition*.

Chapter 8: Partnerships, collaboration and shared services in the public and third sectors

Steve Treece, Colette Dark, Phil Coley, Jeremy Bendall

In this chapter we consider the challenges associated with managing risk within complex and extended public and third sector enterprises, how these challenges are changing and how they impact senior managers and risk practitioners . We look at the key features, attributes and shapers involved in the various collaborative arrangements which affect authorities in these sectors. We also consider the behaviours and culture that support collaboration, whilst delivering effective public services in partnership with third parties. The chapter will explain why developing trust, ensuring clear, effective lines of communication and the management of relationships is vital. We also propose a number of good practice principles, for public sector risk practitioners and managers at all levels to consider and reflect upon.

Public sector risk landscape

The public sector faces a number of specific challenges and complexities, chiefly as a consequence of continuing budget reductions, political pressures, changing demographics and rising public expectations. These challenges define the outcomes it has to deliver, the financial environment in which it operates and further complicate the delivery and value chains deployed to achieve those outcomes. These include:

- Statutory and social responsibilities which the public sector has no choice but to deliver
- The "social contract" by which people trade off rights to their government in return for the expected benefits of greater social order, stability and security
- Increasing public expectations, for example, regarding public health, choice of education providers and ease of access to services
- Operating fully in the public gaze, where 20/20 hindsight is king.
- The assumption that the public sector will always be able to act as "risk bearer of last resort" when major crises occur for events as diverse as assisting a community to recover from a major flood to bailing out a major bank during a financial crisis
- Short term political planning and delivery horizons, creating an environment of seemingly constant change and a public perception of failed or reluctant change
- An over-riding requirement to protect the public purse and to do this demonstrably, which encompasses very specific and public accountability frameworks, for example the National Audit Office and Public Accounts Committee
- Huge exposures to fraud, estimated at £20.6 billion across the UK public sector
- Complex networks of formal and informal service delivery arrangements, which often involve many different partners. For example, the multi-agency approach required to safeguard vulnerable children and adults
- Limitations in the traditional public sector commercial approach and capabilities, including a lack of extensive expertise in dealing with external service providers effectively and on an equal footing
- Fiscal consolidation which will continue to constrain the funding available for public services (at least to 2019) and will require a root and branch review of what services are provided, who is responsible for them and how they are delivered; all with significant implications for the ownership and management of risks
- Financial constraints driving more arms length supply of services and increasing the impetus for "payment by results" and options for more local/community delivery
- Non financial targets are as important as financial targets but their value can be more difficult to assess and manage
- The localism agenda and changes in local/central government relationships

1. Civil Service Reform Plan: One Year On Report - https://www.gov.uk/government/publications/civil-service-reform-plan-one-year-on--2

- Major changes in central government organisational and delivery structures, embodied in the Civil Service Reform Plan[1].

The current state of the public finances requires active and urgent consideration of the redesign of services and the deployment of new delivery models, challenging the fundamental nature and scope of services being provided. This may:

- Result in a blurring and complicating of accountabilities, delivery responsibilities and the interfaces between public and private sectors entailing a significant alteration of existing governance and accountability structures; and
- Produce new and complex relationships which will not always be formally contracted. An increasing emphasis on arms length delivery and "payment by results" brings with it risks of targets and incentives which may result in unexpected and perverse behaviours, leading to poor service delivery, inefficiencies and at the extreme increased levels of fraud and error, with resultant poor public service, lack of value for money and adverse publicity.

The design and commissioning of new delivery models therefore requires a robust consideration of what may be major consequences from changes in service delivery. For example, changes in local/central government relationships, such as those arising from the merger of health and social care responsibilities previously undertaken separately by the health service and local government.

Similarly major central government initiatives such as the move to on-line delivery of all services, as planned in the "digital by default" agenda, requires a wide consideration of potential risks, such as the potential for increasing exposure to cyber-crime and for disenfranchising the most vulnerable members of society who may have more limited access to digital only services.

These new models, however, also present opportunities to rethink and improve service delivery and stop non-essential activities by focussing on the core business of the public sector, sharing costs and risks more widely, increasing delivery capacity (including through access to new markets and market making etc.) and enhancing partner and community involvement.

The Local Government Association publication "Rewiring Public Services"[2], advocates action at local and national levels to transform public services to help communities meet future public needs and aspirations through strong local community leadership by rebuilding democratic participation, fixing public services and revitalising the economy.

These challenges require truly risk based policy setting and decision making, which may well require new accountability and governance structures for decision making, service delivery and assumption/allocation of risk; and better harnessing relationships with the public; all of which are key to the successful delivery of benefits.

This in turn requires a significantly greater focus on outcomes and a reduction in the current emphasis which the public sector places on process. Such a change in focus must also be reflected within risk management and associated assurance frameworks, shifting from a focus on risk assurance processes to gaining meaningful outcomes from these activities. More fundamentally there must be a greater emphasis on true collaboration across the extended enterprise, by building strong long term relationships and avoiding the traditional default to either passive acceptance or confrontation when difficulties occur. There is frequently an over reliance on contract terms as the main (and usually only) control mechanism

Service delivery mechanisms

Service delivery mechanisms requiring examination within the context of public sector value and delivery chain risk and assurance include:

- Shared services within the public sector itself
- Mutuals/co-operatives
- Third sector delivered services
- Private sector delivery
- The movement of responsibilities from the centre to local government for example as in Public Health
- Increasing emphasis on community service delivery and assumption of risk.

We focus on two of these: outsourcing to the Private Sector and the Third Sector

2. Rewiring public services – rejuvenating democracy - http://www.local.gov.uk/web/guest/publications/-/journal_content/56/10180/4047947/PUBLICATION

3. NAO report: Managing government suppliers - http://www.nao.org.uk/report/memorandum-managing-governments-suppliers/

The private sector

Two recent National Audit Office (NAO) reports have focused on the management of private sector suppliers of central government services[3]. The NAO report an estimated £40bn central government spend with third parties in 2012-13 (this is in addition to £84bn from local government, £50bn from the NHS and £13bn with devolved and independent bodies). 25% of this central government spend (£10bn) is estimated to be with 40 strategic suppliers as defined by the Cabinet Office.

They report that:

"The current government, like the one before it, sees contracting out as a way to reform public services and improve value for money. Contracting out can significantly reduce costs and help to improve public services. However, there are several indications that better public scrutiny is needed across government contracting:

- There have been several high-profile allegations of poor performance, irregularities and misreporting over the past few months. These raise concerns about whether all contractors know what is going on in their business and are behaving appropriately; and how well the government manages contracts.
- The government believes that contractors generally have often not provided sufficient value, and can contribute more to the overall austerity programme. But the general level of transparency over contractors' costs and profits is limited. The government needs a better understanding of what is a fair return for good performance for it to maintain the appropriate balance between risk and reward.
- Third, underlying both these issues is the concern that government is, to a certain degree, dependent upon its major providers. There is a sense that some may be "too big to fail" – and difficult to live with or without."

In terms of the need for effective control of outsourced suppliers the NAO also report:

- "The government and public need transparency about performance. Transparency is needed to ensure that no one within the contractor can hide problems and that it is in the contractors' commercial interest to focus on their client's (the government's) needs. This requires more than just the key performance indicators reported to the client. For instance, it also requires public reporting and openness to public scrutiny; whistleblowing policies that encourage staff to report problems up the supply chain; and user feedback.
- The government needs to ensure it is in contractors' financial interest to implement rigorous controls throughout their business. Companies' own control environments will likely concentrate on maintaining shareholder value. Government needs to ensure that it is in the contractors' financial interests to focus their control environment on meeting the standards expected of public service. This involves using contractual entitlements to information, audit and inspection to ensure standards are being met. And it is likely to involve financial penalties, banning from competitions and political fallout when problems are found."

As a specific example, the NAO refer to the contracts that the Ministry of Justice have in place with G4S and Serco for the use of electronic monitoring to confirm that individuals are in their curfew locations at the required times. The NAO report specifically on assurance and control that:

"As with managing contracts, departments retain responsibility for ensuring that suppliers maintain the standards expected. This presents a particular challenge where a contractor is providing a front-line service in an environment devolved from the contracting authority. First, many of the standards expected of all public services are not easily susceptible to contractual specification. It is not possible, for instance, to contract for "integrity" or the "spirit of the law". Second, achieving the standards expected for public service depends to a large degree on the corporate culture, control environment and ethics of the contractor. It is not easy, however, to use contract negotiations to meaningfully assess and set standards for the contractor as a whole.

The recent issues over billing arrangements in the Ministry of Justice electronic monitoring contracts with G4S and Serco highlight the need for a better control framework from departments over service delivery by the contractor."

The third sector

The Third Sector is a specific aspect of the public sector risk landscape which is likely to fulfil an increasing role in the redesign of the delivery of public services, whilst at the same time facing its own specific funding pressures.

This sector comprises Not for Profit and Community Good organisations that have a huge impact on our social wellbeing and economy. The sector includes Charitable Trusts, Incorporated Societies, Public Benefit Entities, and an increasing number of hybrid Social Enterprises characterised by their mix of community and commercial functions and objectives e.g. micro financing/loans to the poor.

Organisational models in this sector have become increasingly complex over the past few decades as organisations moved from reliance on 'old charity' models to new 'business' models. Continued pressure to secure funding in an often highly competitive environment has also translated into the need for:

- much greater collaboration and partnership with like-minded organisations;
- development of hybrid community/commercials models of business; and
- change in governance and leadership practices to recognise the higher level of inter dependency and inter connectedness.

Risk management within this complex environment has had to evolve and a much greater focus is apparent on ensuring:

- Values alignment
- Motivated visionary people with right competencies
- Focussed mission & strategy
- Great discipline in strategy execution
- Optimal organisational structure to deliver results
- Clear roles & responsibilities
- Stable financial, staffing and volunteer base
- Performance incentives that aligned to values and the strategic direction
- Effective risk governance and management with clarity on risk appetite/tolerance
- Strong reputation and brand protection

Collaborative models of the extended enterprise within public and third sector

It is useful to reflect on what is meant by 'collaboration'. According to the Miriam-Webster dictionary, collaboration is defined as

"1. to work jointly with others or together especially in an intellectual endeavour;

2. to cooperate with or willingly assist an enemy of one's country and especially an occupying force; and

3. to cooperate with an agency or instrumentality with which one is not immediately connected."

All three definitions are related to the process of collaboration in business and especially in the non-profit sector where organisations can be seen as competitors for government grants or contracts, or where they co-exist next to one another providing different services to different members of society. However, no matter how collaboration is viewed, the literature time and again suggests the merits of collaboration. A selection of collaborative models has emerged including:

1. **Lead-organisation networks model**: this model considers agencies forming a relationship with one leading organisation selected by public funding agencies to manage the relationships. A government may for example need to deal with organisations that have some local mandate, can represent the local community and can be held accountable through formal structures.

2. **Constellation model:** in considering collaboration, issues often arise concerning how autonomy and accountability is to be maintained and upheld. One solution can be taken from the case of Canadian NGOs. In their efforts to resolve the issue of children's environmental health they applied the 'constellation model'. This model rests on the notion that small teams should address a particular task. These teams focus on the external environment rather than on the partnership itself. Decision-making and leadership rotates between partners according to their skills and the tasks at hand. The underlying task is not strategy-driven but rather opportunity-driven. Once the goal is achieved, or the opportunity is no longer available, these teams become inactive without impacting on the partnership.

3. **Partnering Models:** a partnership can be assessed from different perspectives as there are different stakeholders. However, a specific network should

Figure 8.1: Partnership Continuum Model

be assessed on the outcomes of the specific relationship. Hence, in every partnership it is important to have a clear, achievable goal. Success depends on the fit between the goal and the way to achieve it. As illustrated in the "Partnership Continuum" model in Figure 8.1 below, there are commonly five different types of relationships depending on the goal: coexistence, networking, cooperation, collaboration, and partnerships.

Operating in the extended enterprise – key attributes, features and shapers

We propose a number of ***good practice principles***, for public sector managers at all levels to consider and reflect upon. These are supplemented by ***case studies*** to demonstrate their practical application and a set of tools for public sector managers.

In doing so we have divided the proposed principles under the headings of Attributes, Features and Shapers as described earlier in Figure 1.7 of Chapter 1 and reproduced below.

Attributes

Emphasis is needed on true collaboration and co-operation, by building strong, long term and "adult" relationships, to include:

- Developing an intelligent customer capability in the commissioning and management/oversight of outsourced / arms length services; balancing proportionate and appropriate oversight with constricting interference
- Establishing shared cultures and behaviours across the Public extended enterprise
- Practical application and communication of risk appetite
- Establishing and maintaining effective risk ownership and risk sharing within accountability frameworks
- Partnership working principles in contractual and non-contractual environments

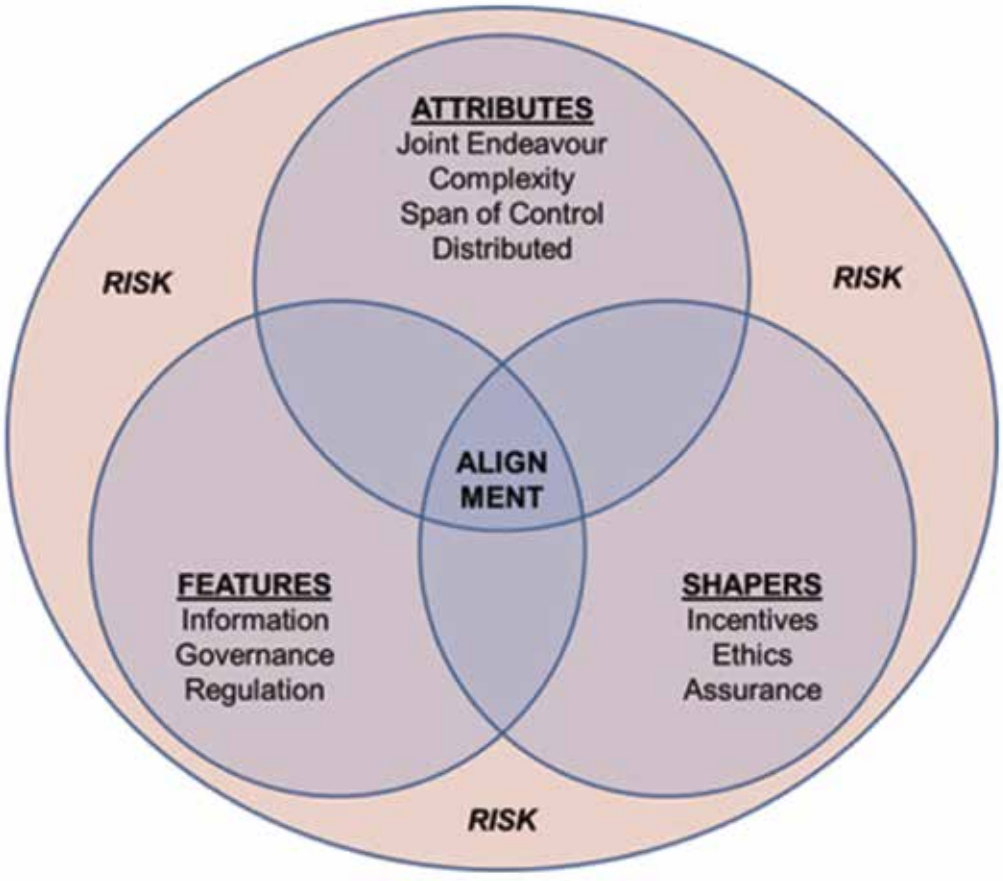


Fig 1.7: Features of an extended enterprise

- Assurance over shared service arrangements
- Contingency Planning – including supplier default/ failure/non performance

There is a need for a strategic overview of the complex network of formal & informal arrangements, which may often involve many different organisations (e.g. several of the child abuse scandals of the too recent past, Victoria Climbie / Baby P etc)

Features

- Changed delivery frameworks may also entail changed risk frameworks requiring consideration of questions such as:
  - o Why do we have this risk?
  - o If the risk is valid who owns it?
  - o If it is a community owned risk, what help does the community need to manage it?
- New delivery models need to be set up within a legislative structure including meeting the requirements of new legislation (e.g. EU Procurement Directive, Public contracts regulations)
- Democratic accountability needs to be maintained and this includes protecting the public purse – this may require some redefinition and resetting of traditional governance and accountability structures, including the roles of scrutiny bodies and regulators
- There is a need to manage (potential) loss of control whilst maintaining the quality and governance of service delivery including the delivery of statutory services (e.g. the Southern Cross Care Homes Crisis)
- risk exposures and assurance mechanisms need to be mapped to gain confidence that the key risks are being managed effectively – there may be a lack of capacity and skills to manage the set up and delivery of these arrangements (e.g. Kerrin Point 1997)
- Reputational risks cannot be outsourced
- Proactive media engagement is required including the management of social media

Shapers

- It is important that personal and organisational values are aligned
- Quality of service delivery needs to be maintained whilst avoiding perverse incentives in delivery of outcomes (e.g. experienced with A4E, G4S) and propriety needs to be managed in payment by results arrangements – both in commissioning of services and ongoing monitoring of delivery
- The Public extended enterprise is likely to be operating within a framework of political "interference" and managers need to be prepared for the likelihood of regular changes in direction at a national/local level
- There is a need for regular horizon scanning including the identification and management of new and emerging risks
- There is a redesign of services and delivery models in central government; creating markets where either none exist or current offerings do not meet requirements
- There are challenges in managing third sector/ community involvement, including practical support when the going gets tough
- Societal risk needs to be addressed
- It needs to be considered whether competition in the public service is always appropriate

Tools, techniques and available resources

One of the central themes of this paper is that the simple application of well-established traditional risk management processes may prove inadequate in tackling the risks associated with the complex extended enterprise. Sadly, this has been demonstrated by a number of headline-grabbing organisational failures. Although, without doubt, it is still necessary to identify, assess, treat, monitor and report on risks, a traditional approach may not be sufficient and the practitioner must be able to understand and analyse the different influences and additional risks presented by the extended model of service delivery.

When dealing with complexity it is probably no great surprise to discover that there is no one tool, technique or resource available to assist in this task.

We suggest that to gain a better understanding of the risks presented, the public sector senior manager, supported by risk practitioners, must be able to explore and understand the key facets of the nature of the collaboration and be prepared to ask some searching questions.

Is the extended enterprise option the right one?

This may be a moot point as the collaboration may already be underway, or the decision made, but consideration of risk is essential and if given the opportunity the risk practitioner has an important role to play in helping to define the strategic direction, identifying and assessing both threats and opportunities from the options available.

A useful resource is **BS 11000-1:2012 Collaborative Business relations**. This describes three phases of a collaborative relationship, the first being 'strategic' within which consideration is given to issues such the objectives and value proposition of the collaboration, resource, competencies and required behaviours, partner selection criteria, an internal self-assessment and the initial risk assessment. (See below, reproduced by kind permission of the BSI[11])

strategic	**Awareness (Clause 3)**	Establish executive responsibility and organisational policy	Identify business objectives and value propositions	Identify and prioritize relationships	establish resources, competencies and behaviours	Undertake initial risk assessment	**relationship management plan**
	Knowledge (Clause 4)	Develop specific business strategy	Establish knowledge management process	Establish objectives, strategy, business case and identify potential collaborative organisations	Establish initial exit strategy	Incorporate relationship managemnt with risk management processes	
	Internal assessment (Clause 5)	Undertake self assessment	Establish collaborative profile	Establish collaborative leadership	Establish partner selection criteria	Establish and implement action plan	
engagement	**Partner selection (Clause 6)**	Nominate potential partners	Evaluate potential partners	Establish partner selection plans	Create joint objectives and negotiation strategy	Select partner	
	Working together (Clause 7)	Establish governance, joint objectives and leadership	Establish organisational structure, roles, responsibilities and processes	Establish performance measurement	Establish joint risk management and exit strategy	Establish contract arrangements	
	Value creation (Clause 8)	Establish value creation programme	Define value drivers	Establish improvement team	Establish learning from experience	Implement innovation process	
management	**Staying together (Clause 9)**	Ongoing management, monitor and measure the relationship	Continual innovation	Maintain behaviours wwand trust	Manage delivery and performance	Manage issie resolution and monitor joint exit strategy	
	Exit strategy (Clause 10)	Develop and maintain joint exit strategy	Establish boundaries for the relationship	Monitor and evaluate changes	Manage business continuity and transition	Evaluate future opportunities	

11. Permission to reproduce extracts from BS 11000-1:2010 is granted by BSI. British Standards can be obtained in PDF or hard copy formats from the BSI online shop: www.bsigroup.com/Shop

Shared Service Architecture Ltd suggests the following decision making route map, referred to as the efficiency matrix[12].

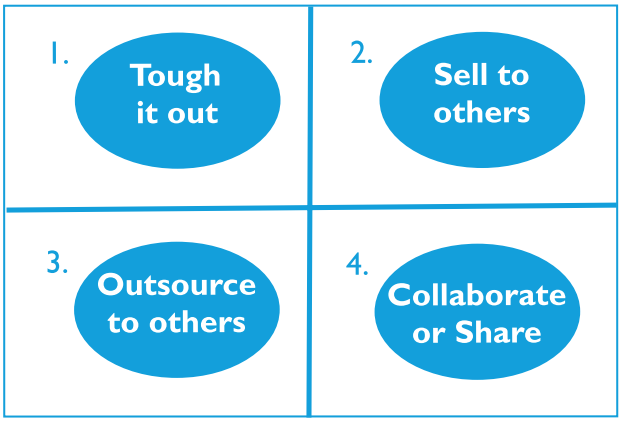


Figure 8.3: Efficiency Matrix

This suggests there are four main options for service delivery available to decision makers in the public sector. These are in order of preference:

1. Tough it out – Although painful, if successful the service will be more efficient and productive than before. Additionally this option has the benefit of retaining complete control over the future destiny of the service.
2. Sell to others – An option open to those who have succeeded in toughing it out. However it will require the development of sales and marketing expertise and a more 'commercial' customer service ethos. The benefit being additional income coupled with retention of control over future destiny.
3. Outsource – To either private or public organisations, who can offer the service but at a lower cost. The majority of control remains within the service and can be exercised through performance targets and monitoring of the contract.
4. Shared services – In effect the public sector version of a merger. It brings with it the potential for significant efficiency gains but requires the surrender of sovereign control.

Some examples of how these different models of service delivery are being manifest is outlined below (Reproduced with the kind permission of Shared Service Architects Ltd)

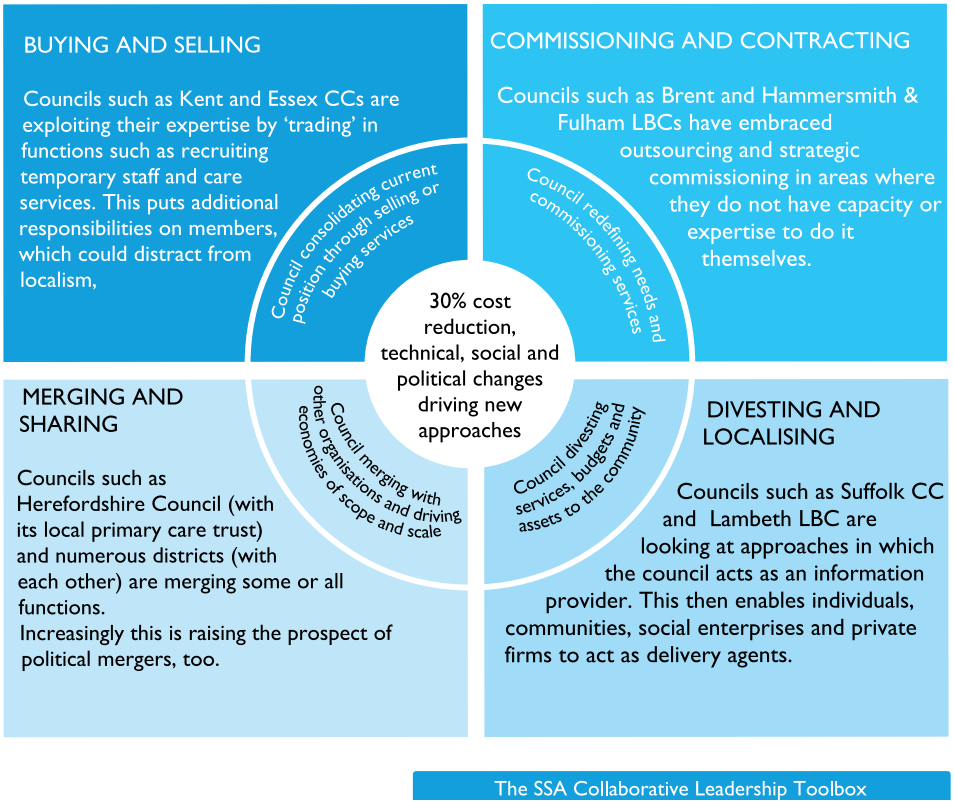


Figure 8.4: Models of shared service delivery

12. (Gatt,E & Wallace,D. (2013) The Highway Code of Shared Services. London. SSA Publications).

Are the organisation and its leaders up to the job?

At an early stage it is also necessary to explore the risks associated with the organisation's ability, in terms of leadership and competencies, to enter into successful collaborative relationships.

In her book on Collaborative Advantage, Elisabeth Lank writes 'because of our collective failure to recognise the connected nature of the organisational world, we have to date largely failed to educate managers and leaders sufficiently in the art of making collaborative work effective' ('Collaborative Advantage: How organisations win by working together ' Lank, E (2006)).

Based on research conducted at Canterbury Christ Church University Business School[13] (Macdonald-Wallace, D (2009) Accelerating the successful delivery of shared services: What skills and knowledge do Members and Officers need to learn?) Shared Service Architecture Ltd has identified the 20 top skills and knowledge requirements for those tasked with leading or project managing shared service arrangements. Reproduced with their kind permission at Table 8.1 is a self-diagnostic tool for practitioners. It is very interesting to note that skills around building relationships, trust, communication, and governance are considered most important with process and knowledge skills only coming into play from statement 13 down.

What are the nature, scale and importance of the collaborations in which the organisation is engaged?

The nature of the collaborative relationship may take on many forms from simple coexistence through to a full partnership relationship where all resources are merged and sovereign control relinquished (as referenced in the "Partnership Continuum" model above).

Moreover, there are a growing number of legal vehicles that can be used to formalise the relationship, each presenting its own governance considerations, operating restrictions, threats and opportunities. To add to this complexity, many large public and third sector bodies are involved in a multitude of collaborative relationships with many different partners.

To operate effectively public sector senior managers, supported by risk practitioners, must ensure that they have:

- an in-depth understanding of the partnerships / collaborations in which the organisation is engaged.
- a reasonable understanding of the legal vehicles involved and the issues and restrictions associated with each type
- a view on the strategic importance of the partnership or collaboration.

For all collaborations and partnerships of strategic importance to the authority consider using the IRM model (Figure 1.7) to explore in greater detail key factors influencing risk in the relationship.

Managing risk and gaining assurance within an extended enterprise

The collaborative model of service delivery is high risk. There are numerous examples of failed attempts or arrangements that have yet to deliver on the promise of the business case.

Gatt & Wallace (Gatt, E & Wallace, D. (2013) The Highway Code of Shared services. London. SSA Publications) suggest three key reasons for such failures:

1. Leaders fail to lead collaboratively and refuse to make changes in their behaviours and ambitions, that are required to deliver a joint project with external partners
2. The creation of business cases that are over optimistic, and their development and project roll-out being under-resourced
3. The project teams are not equipped with the skills and knowledge required, or the authority, to deliver the project.

The common theme running through all the literature is the absolute critical importance of establishing shared objectives and desired outcomes, fostering trust and focusing on relationship management. It is therefore on these 'soft skill' areas that the public sector senior manager and risk practitioner need to focus attention. There are a number of resources that can help.

13. Macdonald-Wallace, D (2009) Accelerating the successful delivery of shared services: What skills and knowledge do Members and Officers need to learn

Table 8.1: Skills and knowledge requirements for leaders (Shared Service Architects Ltd)

SELF-DIAGNOSTIC TOOL	Tick how confident do you feel about your ability in each of the 20 areas		
What skills and knowledge will you require when undertaking this shared service project?	**Highly confident**	**Fairly confident**	**Not confident**
1. The skill of building and sustaining strong trust across leader relationships in multi-partner collaborations.			
2. The skill of creating a positive shared vision, for a project team that may be drawn together from a range of partners of un-equal size or authority.			
3. A knowledge of the key methodologies for supporting decision makers in creating policy for selecting which services to share.			
4. Skills in developing shared vision between a set of partners for a new, better and lower cost shared service.			
5. Skills in developing consensus between a set of partners on the procedures and structure required to deliver a new service.			
6. Skills in developing consensus between a set of partners on the accountabilities and powers in a new service			
7. Skills in building strong trust between key stakeholders during the key stages of a project.			
8. Knowledge of the relevant statutes that will constrain the design of a service(s).			
9. Knowledge of governance model(s) and partnership vehicles that could be considered for a project.			
10. Knowledge of the EU procurement rules that may apply to a project.			
11. Knowledge of the range of relevant tools you can draw on from support and improvement agencies in your sector.			
12. Knowledge of a number of similar projects that have already been completed.			
13. Knowledge of the project methodologies required (e.g. MSP, PRINCE2, Lean, Operational Research, etc).			
14. Knowledge of the Business Process Improvement methodologies you are likely to use in a project.			
15. Skills in drafting clear communication pieces to communicate across a range of mixed stakeholders in a project.			
16. Knowledge of the possibilities and limitations of the range of ICT systems currently used			
17. Skills in estimating return on investment scenarios for the services involved in a project.			
18. A knowledge of sources of financial/performance benchmarking that can be drawn on to inform measurable progress			
19. Skills in designing "invest to save" programmes to enable up-front investment by partners.			
20. The knowledge that you will be released for enough time to be the Shared Service Practitioner or Architect on a project.			

CIPFA document a comprehensive list of 50 shared service risks together with steps required to mitigate them (Sharing the Gain, CIPFA, 2010). The issues highlighted above by Gatt and Wallace are well represented within this list.

BS 11000 Collaborative Business Relationships includes guidance on the development of a relationship management plan and also a relationship maturity matrix that can be used to identify strengths and weaknesses.

Experience would suggest that by aiming for realistic and achievable goals, trust can be built and reinforced. The issues that can put the relationships and trust at risk are personnel change and environmental change. Some solutions to deal with these changes are:

1. Clear documentation is needed
2. A clear review process where reflections are needed on what does and does not work
3. Face-to-face meetings are important
4. Open discussions with a proactive approach are needed
5. Working with the community is important. This is similar to the 'open-source' approach where the idea is to be open about the network and allow people who wish to develop these networks to come to you.

Nuffield Institute for Health has developed a 'Partnership Development Tool'. The tool facilitates an exploration of the views held by the partners in an arrangement to six key partnership principles, namely:

1. Recognise and accept the need for partnership
2. Develop clarity and realism of purpose
3. Ensure commitment and ownership
4. Develop and maintain trust
5. Create clear and robust partnership arrangements
6. Monitor measure and learn.

The results of the assessment graphically illustrate any problem areas and suggest an action plan to address any issues that are surfaced. The tool can be freely downloaded at http://www.doh.state.fl.us/compass/documents/AssessingStrategicPartnership.pd

Case studies

We offer the following case studies as examples of ways that risks in the public sector can be managed on a collaborative basis and how effective assurance on the management of such risks can be obtained.

Central government shared services

In the UK the Cabinet Office has established two independent shared service centres (one is wholly owned by the private sector, and one is a joint venture with government), to provide back office transactional services including HR, finance, payroll and procurement. As these services were previously delivered directly by government departments, UK government Accounting Officers had direct responsibility for, and control over, the delivery of services for which they were accountable for regarding the management of public money. They still have this accountability, without the responsibility for, and control over, the direct service delivery.

An assurance model has therefore been developed by the Cabinet Office Crown Oversight Function to address this situation, which draws upon a number of key sources of assurance:

- An assurance framework has been prepared based on the Three Lines of Defence model. This provides the basis upon which the Crown Oversight Function will assess, in conjunction with customers, assurance that the shared service centre operator is delivering a robust control framework on behalf of their customers and is meeting its contractual obligations.
- An understanding of the risks to the service provided to customers by the shared service centre operator and how these risks have been managed during the year
- The work of the Crown Oversight Function and its contract management forums, including information on any significant non-compliance with service standards on the part of the shared service centre operator or issues that may impact on customers' own Governance Statements.
- A range of audit and assurance work, including:
    - o An industry standard ISAE3402 Type 2 report on the design and effectiveness of on the controls at each shared service centre operator that are likely to impact, or be a part of, the user organisation's system of internal control over financial reporting.

- An annual programme of audits within the Crown Oversight Function and each shared service centre operator to supplement the ISAE3402 reports
- Further management reporting and assurance activity by the shared service organisation

The Cabinet Office has also established a dedicated sub-committee of its main audit committee, which will focus solely on shared services governance, risk management, control and assurance. This Committee will provide an independent view on the adequacy of the assurances received.

Northamptonshire County Council

Northamptonshire County Council manages a complex network of relationships internally and externally to deliver key services. In doing so the Council has adopted innovative ways of working in order to deliver more efficient and cost effective services.

Examples of this include the setting up of the Local Government Shared Service, one of the UKs largest shared ventures, to deliver a range of professional and transactional services to participants and Olympus Care Services, a company wholly owned by the Council providing direct social care services to older people, people with physical disabilities and with learning disabilities. The Council is also developing a number of strategic alliances focussed on shared outcomes and targets with a range of public and private sector organisations and uses market testing services and open sourcing where relevant.

The Council is also focussed on empowering the community to have a greater involvement in the designing and delivery of services.

The Council is constantly looking at new and innovative ways to deliver services through its Business Intelligence Unit which focuses on horizon scanning and identifying 'the art of the possible'. In doing so, business intelligence information is used to anticipate demand and inform how services are delivered.

Across all of this work the Council is clear about having robust assurance mechanisms in place which provide reassurance that key risks are being identified and effectively managed.

All activities are underpinned by a strategy map that sets out the Council's core purpose and its key areas of focus from a customer and community, financial and learning, and growth perspective. As part of this senior managers receive a 'single version of the truth', an overview of key performance indicators including the monitoring of compliance with Statements of Required Practice for areas such as risk management, project and programme management.

The Statement of Recommended Practice for risk management includes risks being identified and reviewed at a service and project level, with a process in place for escalating and reporting on risks to Corporate Leadership Team and Audit Committee as required.

However, strong performance and governance procedures are only part of the story and the Council places great emphasis on building trust and strong relationships with partners who are focussed on achieving shared outcomes and targets. This includes developing a culture where potential risks are openly discussed and dealt with at the time rather than constantly having to refer to contracts. It also includes developing a culture where taking informed risk is actively encouraged on the understanding that this is essential if the Council is to innovate and transform the way that services are delivered. This approach is further supported by the Business Intelligence Unit with its focus on identifying new and innovate ways of working and on providing an environment where ideas can be developed and tested before implementation.

Life Unlimited and Parent to Parent - New Zealand

Life Unlimited and Parent to Parent are two not for profit organisations providing services supporting people with disabilities. Both organisations provide services nationally and are based in Hamilton, New Zealand. In 2008 the organisations formed a partnership in order to bid for and win a new contract with the Ministry of Health for provision of a national information service regarding Autism Spectrum Disorder (ASD).

Key drivers of collaboration

- The single most compelling driver for collaboration was that both organisations had expertise and experience relevant to the advertised tender, however neither would have been particularly strong contenders on their own. The two CEOs recognised that the combined expertise and coverage of the two organisations would come together into a much more compelling proposition
- The two CEOs had some previous experience working together on smaller scale projects.

- Parent to Parent had an existing service providing information on common and rare health and disability conditions, and had in place a network of coordinators employed throughout New Zealand
- Life Unlimited had experience in project management and new service development and a strong and stable financial base.

Developments to date

- Life Unlimited hold the contract with the Ministry of Health
- The working relationship is defined by a Memorandum of Understanding and an annual Service Level Agreement
- The service run by the collaborative partnership is a separate 'brand' Altogether Autism, but is not a separate legal entity. All staff and contractors are employed by one or other organisation
- An operational governance group meets monthly comprised of the two CEOs and key staff
- The partnership has operated successfully over 5 years growing and developing the service.

Key learnings

- Differences in culture between the two organisations have presented some challenges which have required attention and goodwill to overcome
- Requiring staff to seamlessly represent the joint service, Altogether Autism, no matter which organisation they work for
- Working out of two offices in the same city requires specific coordination, understanding and goodwill.
- The operational governance group has a tendency to address operational matters first, and is challenged to maintain strategic focus and leadership.
- The partners are considering whether further collaboration, for example around back office functions, would be beneficial.
- The collaboration has been positive allowing both organisations to benefit and grow – rather than one at the expense of the other.

Conclusion

In conclusion senior managers and risk practitioners working within the public and third sectors are becoming increasingly familiar with the challenges associated with managing risk within complex and extended enterprises. To succeed, the traditional approaches to risk management must be supplemented with a deep knowledge and understanding of the key features attributes and shapers involved in the various collaborative arrangements in which the relevant authority is involved. The authority must adopt behaviours and build a culture that supports collaboration, whilst remaining alert to the need for effective and continuing oversight of the delivery of public services by third parties. Developing trust, ensuring clear, effective lines of communication and the management of relationships is vital.

The Executive, senior management and risk Practitioners should be comfortable they can answer the following:

1. How is due consideration given to both the threats and opportunities presented by the various models available when the initial decision to enter into collaborative working is taken?
2. How has the organisation conducted an assessment of its own ability in terms of leadership and competencies to enter into and build successful collaborative working arrangements?
3. How does the authority have a clear understanding of the nature, strategic importance and risks associated with the various collaborations in which it is currently involved?
4. How does the authority seek and gain assurances that risks are being identified, assessed and managed effectively within strategically important collaborations?
5. Are internal audit services appropriately aligned within the assurance framework; are they adapted to the needs of the extended enterprise; and do they have the necessary scope of work, skills and status?
6. How is effort given to building trust, encouraging communication and managing relationships within strategically important collaborations and is this sufficient?

Chapter 9: Risk capability in the extended enterprise

Amelia Stubbs

The importance of risk capability

In this interconnected world, the capabilities (technical skills, knowledge and leadership competencies) of individuals and the collective group responsible for managing risk, plus the relationships within and outside organisations, can determine just how successful a company is. As a result, many organisations and individuals are now reflecting on the capabilities required for successful risk management, whether for the operation as a whole, or for the individuals responsible for ensuring companies manage risk effectively.

In this chapter we will look at the capabilities and competencies required to manage risk effectively within a company and, importantly, in the more complex world of the extended enterprise. We will also consider the other key roles that are significant in ensuring appropriate management of risk, and the capabilities each group should demonstrate.

Role, responsibility and relationship to risk

Effective risk management is not achieved purely by the independent risk management function. However good they are, they need to work in collaboration with key stakeholders internally and externally to achieve the mature risk culture that companies are now striving to achieve. Each group of stakeholders have their own risk responsibilities, but also their own risk perspective, knowledge and perceptions.

THE BOARD

The role of the Board is to advise and guide the Executive team in their development and execution of strategy. As well as the financial stability of the organisation, they must now consider the risk that the business is subject to, from not grasping commercial opportunities (see 'risk and Innovation' chapter 7) and as a consequence losing market share, to the extension of relationships that could bring the organisation into disrepute. At the same time they should not overstep the boundaries of their advisory remit and interfere in the day to day operational running of the business.

As business complexity has increased and, with it, greater expectations of appropriate governance, the need for a balanced Board with individuals demonstrating the right competencies, or characteristics, is now regarded as a necessity for effective risk management. A recent report published by the Korn/Ferry Institute which asked "What Makes an Exceptional Independent Non Executive Director?" reviewed and updated research on the same topic carried out seven years previously. Along with confirmation that the core characteristics identified in the original report remained, the updated study noted three new essential skills; an understanding of risk, finance and technology. To quote directly from the report, "mastering the complexity of risk is now considered elementary for Boards operating in the post-crisis era".

The core non-executive director characteristics identified in the Korn/Ferry Institute's paper were:

- Independence, courage and integrity.
- Challenging and supportive.
- Thoughtful communication.
- Breadth of experience.

THE EXECUTIVE LEADERSHIP TEAM

In a mature risk culture, everyone is responsible for the risk management of the business. This means doing the right thing and not putting the business at risk in the broadest sense. It is the role of the Executive leadership to ensure this culture is maintained and that all understand their collective and individual obligations. They empower their risk management team to partner the business to ensure the right risk/reward balance is struck but they hold ultimate risk responsibility.

In a mature risk culture, each individual within the business understands their contribution including their risk management responsibilities. Collectively, the organisation is able to think long-term and strategically about the business challenges in the future and to put in place plans to mitigate longer term risk issues through strategic redirection. This is in addition to the risk management processes which ensure day to day risk mitigation.

To achieve this, the Executive leadership needs to think beyond the quarterly financial reports that drive much of the corporate environment. As individual leaders they may demonstrate some of the behaviours, values and competencies detailed in Developing Organisational Capability in risk management (Figure 9.1) designed for the partners in risk management. However, there are additional considerations for leadership in the complex environment created by the 21st century company:

- Evaluating long term value over short term financial gain.
- Ensuring equal value (role/power/money) is placed on commercial risk management and revenue drivers.
- The ability to empower all direct reports to operate in a mature risk environment.
- The willingness to hear and act on challenges.

THE SENIOR RISK LEADER AND HIS/HER TEAM

For the purposes of this chapter we will assume that the senior risk leader is responsible for enterprise risk management as a CRO, head of enterprise risk management or as a head of risk. There are companies where a number of senior individuals collectively take the executive responsibility for independent risk management but an increasing number are appointing one individual to be responsible across the entire organisation or business division. Success requires a desire for understanding and risk maturity on behalf of the Board and the business leaders, and of course, an individual capable of the head of enterprise risk/CRO role. This is a significant and increasingly complex role requiring technical breadth, worldly wisdom, stature and the ability to influence as well as communicate succinctly and with clarity.

The risk team forms the back-bone of effective risk management, working in partnership across the extended enterprise. Organisations require both "high potentials" to succeed bosses when they move on, and well as "high professionals" who constantly ensure the organisation is kept safe.

REGULATORS OR EXTERNAL STAKEHOLDERS

The external stakeholders have their role to play in ensuring risk is managed appropriately and not necessarily only from their own perspective; balance is key. There are now a myriad of stakeholders that a company can and does engage with, and they in turn engage with a host of others, including regulators, customers, suppliers and shareholders.

All can have a profound impact, positively or less so. Where companies are over-regulated, they may seek routes to keep costs down because they have a duty to other stakeholders (shareholders, customers) to maintain costs at a certain level. The outsourcing of processes has been extremely popular but does not always bring the cost savings over the longer term and can certainly increase risks if not managed correctly. Customers can demand increasing cost savings; responding to this and the competitive landscape, companies may choose to adopt a cost-driven supply chain strategy. The results are short-lived but the reputational damage is much harder to fix

Risk management capabilities within the organisation

The risk leader needs to blend technical depth and, increasingly, breadth with the interpersonal and leadership skills to manage the risk team as well as the relationship with internal and external stakeholders. The risk leader relies on the broader team in the delivery of this objective, and they are collectively supported in this by **technical skills** and **knowledge**, behaviours and competencies.

Figure 9.1 explores the capabilities required within an independent risk management team. The core blocks of technical skills and relevant knowledge for the industry and of the company, are shared across the risk function, but some individuals will be deeper experts than others. In developing a mature risk team, a risk leader should look to develop "utility players" i.e. those individuals who have the potential and are capable of moving from one technical area to another. At the same time, the importance of technical specialist should not be under-estimated. They are the guardians of risk management who ensure that frameworks, policy and process remain at the forefront of industry standards and are fitting to the business in all of its operations.

Behaviours and values are the personal traits that should be shared across the function; they operate as the code of practice for risk management and some may have greater emphasis at different times depending on the sophistication of risk management.

The competencies that are required change. As an individual advances through their career and their level of experience grows, other competencies are learnt and developed which enable further progression. As an individual takes on another position, different role responsibilities need different competencies and previous competencies become lessons learnt rather than currently required. Figure 9.1 illustrates competencies most relevant when working as an individual risk manager (Managing Self), when managing a team (Managing Others) and as the risk leader (Managing Enterprise).

Additional capabilities for the extended enterprise

Figure 9.2 considers the factors to take in account and the competencies and values most needed to manage risks in the extended enterprise. Each individual has a role to play, as each will touch the extended enterprise.

When approaching the extended enterprise relationships, what should you consider?

1. Identify and develop a shared sense of ethics and values? Do you have the same approach to risk management and risk culture?
2. A realistic understanding and appreciation of who holds the power? Your company may not have the upper hand, but understanding this dynamic and the impact on your ability to influence is essential.
3. Who gets what out of the relationship? A contract might bind you and dictate the financial terms, but the relationship and consequences of poor decisions have the potential to go far beyond – reputational, operational etc.
4. Interconnectivity dynamics. Partners' industry and economic factors that impact, jurisdictions that they work in (and associated laws), regulators who impact.

To understand, manage and mitigate the above, requires process, contracts and governance. But it also requires an understanding of the human factors that bring contracts to life – behaviours, values and competencies.

To get the best out of any partnership and to maximise open and honest communication, each participant must approach it collaboratively. This is important, and requires a maturity not always present. Approaching stakeholders as a partner will provide the foundation for a productive relationship. Any new partner with a defensive approach

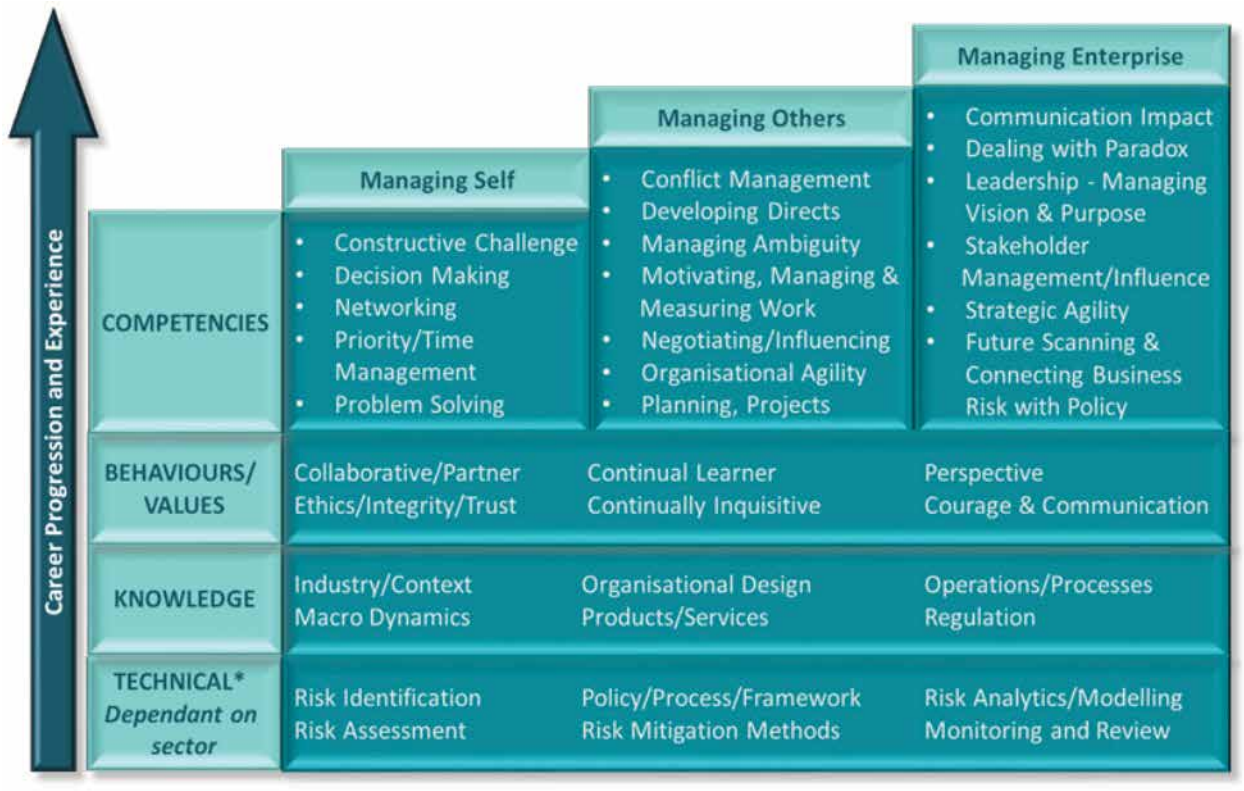


Figure 9.1: Developing organisational capability in risk management

Figure 9.2: risk management capabilities for the extended enterprise

will usually ring alarm bells. In all relationships, as a risk manager, we need open and clear communication as well as the courage to challenge appropriately. This is true too of the extended enterprise and goes hand in glove with a collaborative partnership style if done correctly and with balance. Whilst partnership is key, a risk manager needs to maintain their perspective in order to provide sound judgment on any situation or on the success/challenges of any extended relationships.

Finding a partner that shares your company ethics and values is an excellent starting point, assuming you have the rigour to see past slick marketing. Entering a partnership with a level of distrust or not sharing the same values will likely be a short-term one, ending in dissatisfaction on both sides. A core element of any risk manager, whatever their level, is being continuously inquisitive, not settling for the first answer but quietly persisting until they are satisfied that they have reached the "heart of the matter". In all endeavours, all risk managers must take stakeholder engagement seriously, maintaining and developing relationships, being responsive and collaborative, but also seeking to influence and shape thinking.

Depending on the level and role responsibility, each will have different competencies which could make a material difference to how well risk is managed. We might assume that an individual risk manager could have limited influence and impact. Rather, they are at the coal-face, and through networking will understand what best-in-class looks like and whether the partner shares the same values. They are the foundation of problem solving and decision making; with such information and interaction, they may be the first to see problem risks arising. Whether they are influencing through the relationship they build, the integrity they show, or through their constructive challenge, each individual can mitigate risk within and beyond their enterprise.

As a manager of a team, new skills and competencies are developed. It is the period in a career where the risk manager must become more comfortable with ambiguity as they are now leading a team and a step removed from the day to day detail. As such, they hone their skills in negotiation via developing excellent organisational agility. They must also become adept at conflict management. In the extended enterprise, these four are the most important competencies to develop for the mid-career level. All of these competencies sit within the broader banner of influencing, a key skill for the extended enterprise.

As a risk leader, partnership and the ability to influence become paramount, but so are a number of other core competencies. Dealing with the Paradox, i.e. comfortably dealing with competing ideas and possessing the clarity of thought and communication to navigate between, will help the head of risk deal with competing needs of partners and his/her business. Strategic agility coupled with future scanning are also essential to spot present and future landmines.

Conclusion

In conclusion the Board and risk practitioner should be comfortable they can answer the following:

1. Are the required risk roles across the extended enterprise identified and resourced correctly?
2. Are the risk leaders and team capabilities understood and aligned to the challenges of managing risk across the extended enterprise?
3. Does the Board understand and periodically review the risk capabilities of its organisation?

Chapter 10: Risk communication in the 21st Century extended enterprise

Andy Bulgin

The importance of risk communication

This chapter provides a definition of risk communication, and considers how best to avoid language and terminology which might impact on communication effectiveness. Through the chapter we will review the characteristics of 21st century extended enterprises which make effective communication challenging and consider ways to utilise recent social media channels as effectively as possible to create an effective risk communication strategy.

Communication has always been an imperfect science, reliant on a common appreciation of the meaning, implication and tone of language being used. Misinterpretation of messages will impact the performance of even the simplest of corporate entities. This impact is likely to be magnified in a complex, less formally structured 21st century enterprise.

Risk messaging is a vital sub-set of corporate communication, enabling enterprises to understand their risks and achieve at least a degree of risk resilience. To be effective, it needs to have exactly the same characteristics as other model communication – clarity, simplicity and unambiguity. It also needs to take into consideration differential risk perception and risk terminology, and common statistical misinterpretation.

As enterprises have become more complex and diverse, the ability to ensure common linguistic understanding and interpretation has become increasingly difficult to achieve. Yet, the need for clarity of communication has become ever more paramount; without it, there is unlikely to be uniform purpose, shared systemic beliefs and ethics, or a means to achieve assurance for all stakeholders.

The effectiveness of any communication policy relies on its ability to get its messages across to all relevant stakeholders in a consistent way. Stakeholder mapping should identify those who need to be communicated with but care must be taken to ensure key people who sit at the boundaries of an enterprise network are also considered.

The world is now swamped with information from both official and unofficial channels. This has made people both cynical and desensitised. Modern communication needs to take this into account and ensure that messaging is even more frequent, consistent and focuses on ethical, as well as financial, performance.

Communication in the 21st century has been further complicated by the arrival of a host of social media channels. These provide the capability for anyone to comment immediately, and indiscriminately, on any event. The inability of an organisation to control reporting on any given incident greatly reduces its capability to manage the incident effectively. This applies particularly in a risk context and means that enterprises must understand and embrace social media as part of their communications protocol to ensure resilience.

Context

"The single biggest problem with communication is the illusion that it has taken place."

– George Bernard Shaw

The importance of clear, succinct and frequent communication remains as relevant in the 21st century as it always has. However, the complexity and diversity of modern business enterprises increases the chances of communication misinterpretation, and breakdown. In addition, enterprises are now faced with a bewildering variety of new communication channels, many of which are difficult or impossible to control. These issues must be reflected in enterprise communication protocols, particularly in the area of risk specific communication, which forms much of an enterprise's ability to protect itself against potential disaster and subsequent reputational damage.

What is risk communication?

Risk communication is an essential sub-set of any corporate communication policy, but few recognised risk management standards attempt to define the process in detail.

The UK Risk Management Standard, issued by AIRMIC, ALARM and the IRM in 2002, offers no more than a simplistic description of the process, defining it as the " Exchange or sharing of information about risk".

The ISO 31000 Risk Management standard 2009 does not even define risk communication separately but as part of the process of consultation:

"Continual and iterative processes that an organisation conducts to provide, share or obtain information, and to engage in dialogue with stakeholders regarding the management of risk."

This definition, however, at least picks up on the need to talk to stakeholders and to make this process an iterative one, but still does not offer a guide as to how to do this, and what makes risk communication effective.

Certain entities have attempted to enhance the basic definitions of risk communication within Global risk standards. The World Health Organisation, for example, offers a concise, but arguably more complete, process summary in a single sentence:

"An interactive process of exchange of information and opinion on risk among risk assessors, risk managers and other interested parties"

This definition highlights a number of desirable elements in the risk communication process:

- It should be an interactive, reciprocal activity, moving away from defined rules and moving towards trust, collaboration and shared values.
- It needs to take into account that opinion, as well as factual information, shapes stakeholders' risk views.
- It should acknowledge that communication extends beyond risk experts to all other interested parties. This means that risk messaging needs to be clear, non-technical if at all possible, and unambiguous.

Factors affecting risk communication

Establishing a viable process for risk communication is important, but knowing what to say to each stakeholder group, and how to say it, is even more vital. The nature of your messages will depend on a number of key factors, such as:

Risk language

Despite many attempts to define risk terminology, there is no universally recognised lexicon of risk either within or outside of the risk management profession. Extreme care therefore needs to be taken when communicating on risk issues to ensure the language used is commonly understood and interpreted by all stakeholders.

Misunderstanding can arise at the most fundamental level, such as when people confuse the terms "risk" and "consequence". It can also occur at a more technical level when communicating to a multinational stakeholder group; there is a real danger that commonly used technical expressions can have different meanings in different countries.

A major European manufacturer took the decision to sell off its own storage facilities in France and replace them with rented warehouses. Included within this decision was agreement that goods stored within these rented warehouses would be insured by the warehouse owners. Terms and conditions of the insurance were vetted by the manufacturer's risk department and deemed to satisfy corporate requirements. Included within these terms and conditions was a general exclusion for Acts of God.

Several months later, significant amounts of stock were stolen from 3 warehouses by armed robbers. When the European manufacturer tried to claim for these losses, they were informed that armed robbery constituted an Act of God as interpreted by the French Insurer, and was therefore not covered.

Risk perception

Concepts of what constitutes an acceptable or unacceptable risk or consequence vary from country to country. For example, in many parts of the developing world death or injury are seen as a sad but unavoidable consequence of travel. This attitude can be further exacerbated by cultural belief which may imply a degree of fatalism to whether things happen or don't happen.

This fatalistic attitude is unlikely to be tolerated in the developed world. Indeed, most companies will be under considerable pressure from stakeholders to demonstrate that injury or loss of life whilst travelling on business is unacceptable. Thus, when entities in the developed and developing world combine in an extended enterprise, there may well be a conflict of interest on what does and does not constitute an avoidable, or at least controllable, risk.

If one element of the extended enterprise has management control, then it will be possible to enforce their approach to risk through mandate. However, if such control does not exist, then the communication will need to rely on a system of shared enterprise ethics and beliefs to be effective.

Statistical misinterpretation

A large proportion of the population, including the media, do not understand statistics and what they mean in terms of relative and absolute risk. This can cause misinterpretation of messages and produce unwanted side effects.

In 1995 general guidance was issued to doctors in the UK that use of the third generation combined oral contraceptive pill increased the risk of venous thrombosis by 100%. Alarmed by this seemingly huge risk increase, many women stopped taking this type of contraceptive pill. The following year an additional 10,000 abortions occurred, many of which were believed to be related to the reduction in use of the contraceptive.

The study on which the initial guidance was based found that taking the combined oral contraceptive pill increased the incidence of venous thrombosis from 1 woman in 7,000 to 2 in 7,000. The relative risk is indeed a 100% increase but the absolute, or underlying, risk is considerably lower.

This misinterpretation of relative and absolute risk is particularly common in medicine, but it certainly occurs in other risk issues. Particular care, therefore, needs to be taken to ensure that a risk message is sufficiently clear to allow all Stakeholders to interpret it correctly and to understand the absolute level of risk being faced.

Characteristics of 21st century organisations that change the way we need to communicate

The previous chapters in this study have highlighted the complexity faced by businesses in the 21st century and how best to manage it from a risk perspective. There are clearly a number of features of 21st century enterprises that influence how, how often and to whom we communicate:

Uncertainty renders many traditional management systems redundant

The introduction to this paper succinctly outlined the difference between simple and complex management systems. Much of this difference is contained in the concept of simple enterprises having rules and certainty and complex enterprises replacing these with uncertainty, controlled by principles, behaviours and ethics. Within the complex environment, communication can no longer be only mandatory and rules-bound; it frequently needs to be replaced by messaging which clarifies individual responsibilities arising from shared desired behaviours and ethical stances. Finding such common ethical ground is often a challenge in supply chains still dominated by cost issues.

Communication channels are not fixed, or controlled

The rapidly evolving structure of enterprises in recent years has changed the accepted rules and routes of communication. In a vertically integrated enterprise, rules were typically used to ensure common purpose. Some of these rules would apply to who was allowed to communicate corporately, what they were allowed to say and when such communication could be made. It was not uncommon for all corporate level communication to be subject to edit by an overall corporate communication function.

As businesses moved from vertically integrated enterprises to partnerships, the ability to control activities, including communication, became more of a challenge. There, therefore, needs to be a reappraisal of:

- Who is allowed to communicate and through what medium
- Who, if anyone, has right of veto for any given communication in an enterprise
- What are the key messages that should be given in any communication. This applies to content, tone and language as all of these will impact your stakeholders.

Such considerations apply for all forms of communication. They are, however, likely to be critical for risk communication, particularly in crisis response and management situations.

Geographical distance between network partners is significant

It is a function of most modern companies to continually move their global resources networks to achieve the most cost-effective production or service. Whilst this frequently improves upfront costs, it will almost certainly create underlying risk issues:

- Offshore services are often located in places where those providing them speak the corporate language (European, Scandinavian etc) as either their second or third language. This inevitably increases the risk of misinterpretation of discussions and/or agreements with the commissioning company.

- Partners operating in different time zones will often introduce a communications timing issue that can be critical when dealing with incidents.
- It is hard to know real time what is going on in a geographically disparate supply chain.

Outsourcing is the norm

Most modern businesses have a mixture of formal and informal agreements within their business activities, arising from the variety of partners they deal with. Much of this has been driven by the desire to save money through outsourcing of all activities that are not deemed core to a company.

Outsourcing is ostensibly cheaper but carries with it a substantial risk of loss of control; there is frequently a confusion of role sorts:

Traditional supply chain models had a clear, hierarchical structure with larger entities buying components or services from subsidiary organisations that were usually not direct competitors. Control of the supply chain usually rested with the entity buying the components or services.

Modern day arrangements frequently lack this kind of hierarchical approach.

Samsung first supplied Apple in 2005. What began as a deal for delivery of flash memory was subsequently extended to include supply of application processors for a variety of devices. By 2011, Samsung was providing 26% of the components for the Apple iPhone, as well as a significant proportion of other components for the iPod and iPad.

When the relationship first developed, Samsung were not seen as competitors to Apple in the mobile phone market. This perceived non-competition, and Samsung's willingness to invest more than $10bn in capital investment and R&D made them the ideal trading partner for Apple.

Samsung, however, clearly gained from the relationship, not only from Apple's $8bn plus purchase of parts per annum but also from insight gained into Apple's marketing strategy. The relationship also allowed Samsung to support their own business strategy by giving them sufficient manufacturing scale to ensure efficiency of their own production.

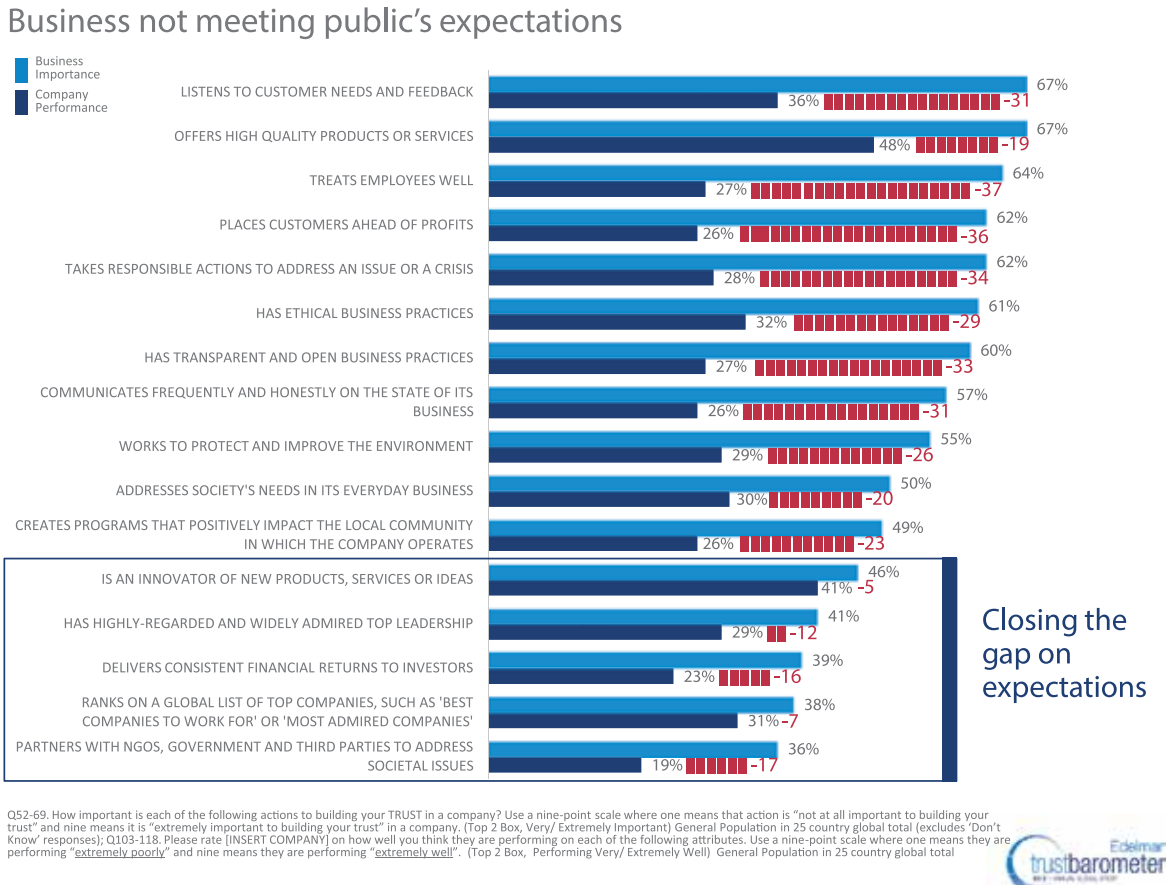


Figure 10.1: Edelman Trust Barometer (reproduced with permission)

Samsung has now become the global leader in mobile phone supply, partly through the creation and sale of handsets similar to Apple's iPhone. This change in the supply chain hierarchy has inevitably led to competitive tensions and ultimately legal action by both parties. However, the relationship remains intact in 2013 and it is unlikely to change whilst Samsung remains the global leader in supply of key components for Apple.

Defining and communicating risk in such a complex supply chain structure is clearly extremely difficult, as risk to either partner is likely to change frequently.

Public perception and priorities

Ethics has become a key concern in consumer purchase decisions

The Edelman Trust Barometer measures attitudes about the state of trust in business, government, NGOs and media across more than 30,000 participants in 25 countries. The results of the 2012 survey (see Figure 10.1) show, amongst other things where companies are not meeting public expectations on key business performance issues:

Key perceived weaknesses are identified as poor customer feedback response, failure to adopt an open and ethical stance to business and failing to treat employees fairly. Maintenance of quality of product/ services is still key but its importance is seen as only equal to these other ethical issues.

Consumer conviction will only come from extensive messaging

The Trust Barometer also looks at how often an entity needs to communicate a particular message to overcome public scepticism arising from information overload (see Figure 10.2):

Companies require consumer trust to remain successful. This will only happen with provision of evidence of focus on these key ethical/ soft issues. This has implications from a risk communication angle:

- Both internal and external proactive communication needs to focus on satisfying the public's ethical demands, as well as continued financial success.
- The scope of communication needs to be expanded to include all Stakeholders which, by definition, extend well beyond shareholders.
- The frequency of communication needs to be greater to overcome the public's natural scepticism for corporate messaging.

Stakeholders' corporate interest goes well beyond financial performance

Traditionally, a company's external communication was primarily aimed at shareholders and analysts, and focused on financial performance. The complexity of the 21st century enterprise makes such communication too one-dimensional; there is a need to address the concerns of all stakeholders, both internal and external,

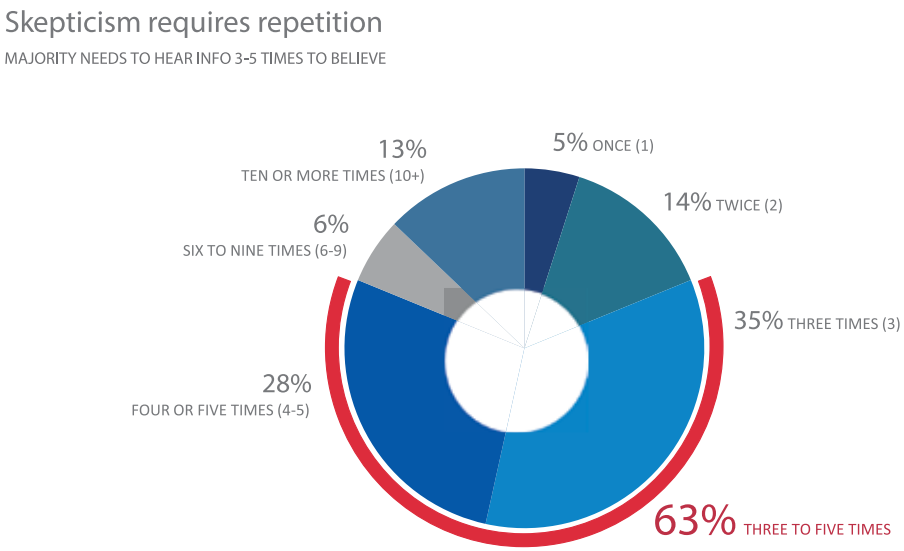


Figure 10.2: Skepticism requires repetition (reproduced with permission)

on a variety of topics linked not only to financial performance, but also to environmental, social and community impacts.

The rise of social media: "anytime, anyplace, anywhere"

Martini's iconic advertising line from the 1970s is an apposite description of the 21st century communication landscape. A recent survey showed that Facebook now has more than 1 billion registered users, an increase in membership of more than 80% since 2011. Twitter has more than half a billion users with around 130,000 new users signing up each month. Tumblr, the blogging site, has an estimated 300 million users and LinkedIn, Pinterest and MySpace all have between 70-110 million registered users. It is estimated that social networking now reaches 1 in 4 of everyone on the earth and this is likely to continue to increase.

Despite this global saturation, there is a tendency to dismiss Social Media as irreverent and irrelevant; as one commentator recently described it "a virtual mirror for narcissists and a meeting point for the terminally vacuous."

Although much of social media content may be rumour and gossip, it is having an increasing influence in the modern world. What does this growth of social media mean for the 21st century entity?

Speed of reporting

News stories now break within minutes of an event occurring. Video footage of a disaster was first posted on Twitter in 2009 when a ferry passenger tweeted a picture of a stricken US Airlines plane making an emergency landing in the Hudson River. Since then, twitter has been responsible for a number of notable news coups, perhaps most famously breaking the story of the raid to kill Osama Bin Laden.

Twitter, and other social media vehicles, now allow everyone with an internet connection to report real time on issues as they occur. This presents companies with the challenge of monitoring all news stories 24/7, speedily assessing the validity of them and responding appropriately should the story affect the entity or its network.

Reliability of reporting

A number of pictures were tweeted during the 2011 London riots, allegedly showing the London Eye on fire. (See http://www.theguardian.com/uk/2011/dec/07/how-twitter-spread-rumours-riots)

The fact that the Eye is made of steel and is unlikely to burn didn't prevent this image from being accepted at face value and retweeted many thousand times. Such images and messaging are symptomatic of the indiscriminate nature of social media. This has significant implications for the communication approach of the modern enterprise. It is almost impossible to prevent inaccuracies and scurrilous rumours from being spread electronically at an extremely fast pace; the communications policy in place needs to know how to track these, and respond appropriately.

Positive and negative influencing power

Despite the unreliability of much reported on the web, there is still quite clearly the power to mobilise many into swift action, as seen in the London riots of 2011. The Metropolitan Police (MPS) recognised this power but admitted that they did not have the capability to control or influence it. In their Strategic Review into the disorders, they stated: "The ability of gangs to co-ordinate widespread crime during the riots by using the Internet and other means of digital communication was a new phenomenon. However the MPS had not encountered an incident with such fast-moving coverage and its system to co-ordinate and prioritise the collection of relevant intelligence was tested to the limit. The MPS could not comprehensively monitor social media in real-time and was therefore not in a position to be moving ahead of events"

Lack of knowledge and understanding of the power of social media means it is often only seen as a negative force. However, the London riots provided a perfect further example of the positive power of the internet. Immediately after the riots a Twitter campaign was organised by artist Dan Thompson to ask residents to help with necessary clean-up operations. Within hours, many thousands of people turned up with brooms, dust pans and cleaning equipment to speed the return to normality.

Understanding how Social Media works is therefore key to using it to your best advantage.

Components of a risk communication plan

Proactive, or planned, communication obviously offers the enterprise the chance to say what the want to say and to direct it to a chosen audience. To maximise the chance of success and protection of corporate position/ enhancement of reputation, there are several key elements of a plan:

Cross-enterprise communications approach

All enterprise communications need to be consistent in tone, language and messaging. There therefore needs to be agreement with all key stakeholders as to who can communicate and what they can and can't say. Guidance on this is likely to come from the entities within the enterprise that have real, or perceived, power. However, it is unlikely that autocratic guidance from such entities will work; there needs to be a collective sympathy, or belief, in the nature of communications in order for everyone to follow such guidance.

Stakeholder identification

Stakeholders can be identified from a number of potential viewpoints; the example in Figure 10.3 below looks at things from a Corporate Social Responsibility perspective but other models can be adopted, as described in earlier chapters of this study. Whichever identification approach is used, the important thing to ensure is that all potential stakeholders are included.

Communications plans tailored to individual stakeholders

Once the groups of stakeholders have been identified, an individual communication plan needs to be devised for each one, specifying:

- The nature of your relationship with each Stakeholder
- The relative powers of each Stakeholder
- Each group's concern/ risk appetite
- How aligned/ unaligned are you currently with each stakeholder
- How to ensure maximum alignment (nature of communication, format, frequency etc.)
- What communication media you use to engage with each stakeholder

The objective of such stakeholder engagement is to enhance corporate perception, credibility, image and, ultimately, reputation. The complexity of modern business may well make the stakeholders' positions unclear. Clarification of position, common understanding and trust will therefore be the purpose of communication.

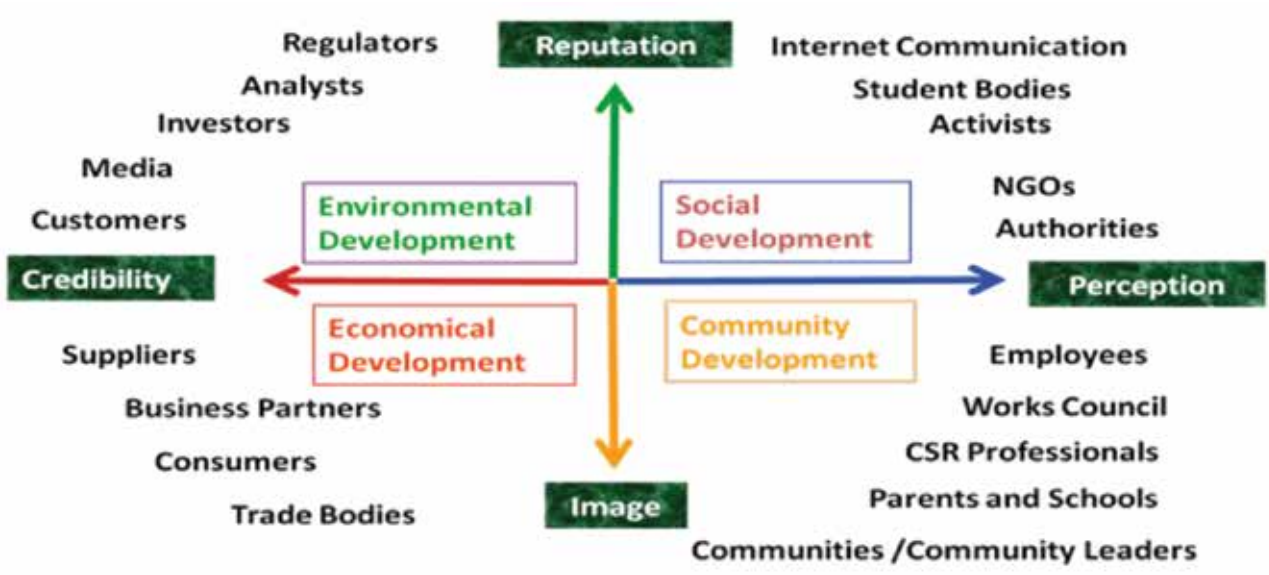


Figure 10.3: Stakeholder identification

Control of communication within the business network

The complexity of modern business and the myriad opportunities for instant, unofficial communication from everywhere make control extremely difficult.

Social media control is perhaps the single biggest issue in communications control. In theory, it should be simple to conceive a strategy to ensure all stakeholders only use social media in a controlled way. In practice, this ignores the fact that personal and business social communications have become almost inseparable. Most organisations now use social media for corporate purposes. They therefore provide employees with communications devices to achieve this and expect it to be part of normal business activity. In an ideal world, people should have separate accounts for work and leisure. In reality, this separation is difficult to achieve and attempts to restrict social media activity could be interpreted as interference with personal freedom of speech.

The confusion of personal and business messaging also opens up a further risk issue for companies. If an employee is sending messages on a company device, is the company vicariously liable for any legally damaging comments contained within such messages? To date, no such legal action has been pursued, but it is possible that it will happen sometime in the future.

Ideally, we should agree with all stakeholders:

- Who owns the risk at any stage in the business network
- Who is allowed to comment on risk issues
- Which media channels are acceptable for such comments

Such agreement is unlikely to come from a rules-based approach; it will rely on creation of trust, and agreement of common goals and ethics.

Incident response specific communication

21st century communications channels provide a constant stream of corporate information, both positive and negative. The need for effective incident response has therefore become even more paramount. The basic incident response messages to the general public when an issue arises are not fundamentally different in the 21st century. However, the speed with which stories break, and the lifecycle of a story are much changed, and these factors influence how, and with whom a company or network must communicate.

In March 2010, Nestle were targeted by Greenpeace via a social media campaign. Greenpeace had found that Nestle were sourcing palm oil from Sinar Mas, an Indonesian supplier, who, it claimed, were acting unsustainably in clearance of forest.

Greenpeace created a gory video on YouTube, parodying the companies' advertising slogan, "have a break, have a Kit Kat". In the video, an office worker opens a Kit Kat and is seen biting a finger which turns out to be the severed digit of an orang-utan.

Nestle initially demanded the video be withdrawn from YouTube. It also removed negative commentary and reposts of the video from its own Facebook page. Despite these attempts to control the issue, the video was re-posted on both YouTube and Vimeo, and more than 250,000 people viewed it in the space of four days.

Nestle's attempt to control the comments on their Facebook page was very badly received, with numerous public comments alleging censorship to hide the issue. This exacerbated the situation still further and forced Nestle to:

- Suspend sourcing of oil from Sinar Mas
- Join the Roundtable for Sustainable Palm Oil
- Create a new social media strategy through the appointment of a global head of digital and social media.
- Set up a "digital acceleration" team to monitor social media 24/7 and train executives in the management of social media communications and digital marketing.

The lessons learned from this issue are relevant for all 21st century organisations:

- Recognise that your critics are your stakeholders and engage with them
- Do not attempt to shut down social media; it will not work and will, almost certainly, lead to further negative exposure
- Ensure effective communication training throughout the organisation
- Monitor communication 24/7

Social media as a tool for effective disaster management

The upside of the speed of social media is that it can greatly assist with disaster management. In September 2011, around 5m Americans on the West Coast were temporarily without power. San Diego Gas & Electric used twitter to respond immediately: "We understand power is out, we are working on the cause and solution. We do not have a restoration time yet". Over the next 12 hours the company used #outage to provide updates and tips on both safety and protection of house and home, and the company's efforts to restore power. This communication process was backed by website information, radio and TV broadcasts and press conferences. This co-ordinated, blanket communication approach greatly reduced collateral damage arising from the outage and enhanced San Diego's Gas and Electric's reputation substantially.

Whilst Governments and international relief agencies have clearly bought into this social media based approach to disaster management, commercial enterprises appear more hesitant to proceed down this route. Perhaps their reticence is related to social media issues encountered by companies such as Nestle and an intrinsic mistrust of something which is not completely understood.

What is clear is Facebook, Twitter and other media communication sites are viable disaster response mechanisms; appropriate tone of messaging, and a willingness to engage with stakeholders are probably the keys to ensure lack of negative response from the general public.

Conclusions

This chapter has considered the characteristics of modern business and the global communications landscape. In conclusion the Board and Risk Practitioner should be comfortable they can answer the following:

Do you understand the risk communications within your supply chain/network?

- The inherent complexity of both business and communication renders a traditional, rules-based risk communication approach redundant; what is needed is a softer approach, based on understanding your network partners, to create agreement and trust in management of risk.
- Risk communication has always been hampered by differential risk perception and risk terminology, and common statistical misinterpretation. The impact of these issues has been magnified by the increase in complexity and uncertainty in the 21st century enterprise.
- The geographical and cultural disparity of network partners makes clarity of communication critical; ensure any risk agreements are clear and unambiguous.
- if there is any doubt as to who manages a key risk, it might be better to try to avoid it rather than to outsource it.
- Whilst an ethics- led risk communication route is likely to work well, there is still the possibility of certain supply chain partners refusing to accept risk responsibility through lack of financial reward.

Do you understand the risk communications to your stakeholders/ the general public?

- Identification of all stakeholders is essential.
- All corporate communication, including risk communication, needs to be repeated more frequently to overcome modern day cynicism.
- Social media is now an integral part of modern communications and needs to be embraced by businesses as such.
- Do you have an effective communication response capability?

- The indiscriminate, uncensored nature of much on the internet is potentially damaging, but it can be harnessed to provide immediate response in crisis situations.
- The key is to understand the characteristics of each media platform and ensure that your messaging uses appropriate language and behaviour to engage with the majority of your stakeholders.

And finally, communication of any description has always, and will always, depend on accuracy of language for effect. James Thurber, a citizen of the 19th and 20th centuries, said this:

"Precision of communication is important, more important than ever, in our era of hair trigger balances, when a false or misunderstood word may create as much disaster as a sudden thoughtless act."

There is no doubt that his words still remain relevant in the 21st century.

Chapter 11: Standards and assurance

Daniel Roberts, Steve Treece

Is the current assurance model broken for the extended, 21st century enterprise?

From the perspective of the extended enterprise, the argument can be made that the existing assurance model is too expensive for the levels of assurance that can be achieved or provided. In addition, elements of the extended enterprise are hamstrung by too many assurance standards, overlapping standards, and individually inadequate standards. This presents the purchaser of goods or services with a too-complex environment, and the provider of goods or services with sets of overlapping and potentially conflicting assurance standards requested by their customers. Finally, each purchaser is, in most cases, also a supplier, creating a spider's web of interlinked set of relationships, each assured by overlapping or even potentially mutually incompatible standards.

Certainly there are examples of enterprises that have implemented assurance environments across their extended enterprise. In these cases, the primary drivers have been extreme negative events, resulting in a need to be able, as a survival factor, to demonstrate consistent business practices across their web of relationships. The very nature of the Extended Enterprise - the "Extended" element, means that there may be multiple "steps" between suppliers, customers, and other interested stakeholders. Each "step" represents the potential for additional levels of opacity, and greater opportunities for the assurance provided to be less meaningful. In addition, the cost burdens of requesting and reviewing the assurance provided increases significantly with each "step" away from the assurance requesting element of the Extended Enterprise.

Why require assurance?

Before progressing into discussion of the current assurance model and why it may be broken, let us look at why the Enterprise and the Extended Enterprise seeks assurance. The largest "Enterprises" have not been monolithic for most of a century, with parts of their production, marketing, distribution and sales effectively outsourced to providers and sales channels around the world. The difference over the past two decades has been the globalisation of the Extended Enterprise, and the extending of both supply chains and the steps in the supply chain.

This has meant that an Enterprise, small or large, could be sourcing product content from multiple continents and a large number of countries, each with its own laws, cultures and constraints. In addition, the actual source of the goods or services could be multiple contractual steps away (degrees of separation) from the final purchasing enterprise. Having confidence that the inputs sourced meet quality standards, are delivered on time, and that reputation risk is being managed are critical. Assurance, via contract requirements, has long been acknowledged as providing only the minimal level of comfort to management and stakeholders.

For example, product carrying a company's logo and brand promise could be purchased by a consumer (individual or corporate) of the product without the delivered product every actually "touching" an actual employee or representative of the company. This brings to mind that wonderful expression "so what could possibly go wrong here"?

Unfortunately, the past decades have shown us only too well what could go wrong. Misinformation can destroy a brand almost as badly as truthful information about the brand. Banking used to be a respectable profession, running shoes used to be linked to superstars (and still are), and horses were for courses, not for dinner.

What is assurance?

In its simplest form, assurance aims to give confidence, backed up by demonstrated compliance with a standard, that what you are being told is happening, is actually happening. Assurance is provided by independent third parties (or independent internal functions such as risk management or Internal Audit), and should be based on a review of processes, systems and controls. Ideally, such reviews and results can demonstrate compliance with one or more standards.

Fundamentally, assurance is the process to help executives and stakeholders sleep at night.

Is the assurance model broken?

Businesses seek assurance covering a number of aspects of their processes, systems and outcomes. They also seek assurance that business partners' processes, systems and outcomes will both achieve objectives and not expose either business to risk beyond what has been agreed to be acceptable. Businesses provide assurance to a number of external parties, including their shareholders, financial institutions and funders, regulators and of course customers. The core business determines the standards that are most applicable or of greatest importance to achievement of its goals.

The Extended Enterprise (our "business" and its key stakeholders) needs to be provided with assurance from and by various elements of that Extended Enterprise. Equally, the business needs to be providing assurance to customers, suppliers (for data security for example), regulators and the wider stakeholder community.

The ability to receive and provide assurance is undermined by the wide range of standards for assurance, and the selections of standards (applicable to that business) by each participant in the Extended Enterprise. In addition, each standard covers only a defined subset of business processes and systems, and therefore provides limited coverage. To achieve complete coverage, multiple standards can be required.

It is worth noting that while Control Risk Self-Assessment (CSRA) can be an effective tool for the identification of risks and monitoring of the effectiveness of controls, it is not a methodology that by itself can provide assurance "multiple steps" away in the "extended" element of the Extended Enterprise.

Steps or level:

Each enterprise is at the centre of its own world-view. Imagine off to one side are customers, and beyond them, their customers; on the other side, suppliers and their suppliers stretching off into the distance.

From a practical and cost perspective, it becomes difficult to audit, request or require assurance from more than one or two steps away, and difficult to justify providing independent assurance reports to all customers regardless of how many steps they are removed. Each assurance report, each customer audit, each mandated standard introduces costs, to the provider and to the requester.

Therefore, it is relatively common to request or provide assurance one step away, while the Extended Enterprise by its very nature is a multiple step environment.

"Audit" looks only at the enterprise and usually does not delve deeply into the multiple levels of the supply chain.

The annual statutory audit provides limited if any assurance to the business, as such activity is specifically required to provide the investor (and regulator) with confirmation that the financial statements provide a true and fair representation of the historical financial position of the entity. Therefore, the audit has an inward looking, specific content area focus (financials) and does not cater for the extended enterprise, supply chain or wider stakeholder community needs for assurance.

Vendor assessments look at the next level

Vendor assessments provide a level of assurance, subject to the limitations (cost, time, and detail) of the review process and breadth of reviews. While companies can prioritise which vendors will be subject to review based on criteria such as criticality to the business, retention of privately identifiable data on clients, regulatory compliance, health and safety, or any of a range of other factors, selection and scheduling of reviews will result in a certain level of residual risk being carried by the company.

Vendors look at their next level

Unfortunately this means that in too many cases the company needs to rely on vendors to perform assessments of their vendors; a never ending chain of expectations, with an almost guaranteed result of vendor assessments either not being performed at some stage, or of a critical supplier being missed from the assessment schedule.

Standards

Once the decision is taken to request or to provide assurance, the next major question is what type of assurance to provide - what standard to demonstrate compliance with. The standards selected should be linked to or based on the types of services or products purchased or sold. And here is the problem; there are simply too many overlapping standards.

For example, where the supplier is providing a financial service such as payroll processing or custody services,

the Enterprise may wish to see evidence of independent certification based on ISO 27001 (for IT Security) and a SAS70/SSAE16 report on controls over financial processes and reporting. Likewise, if the provider is producing components, the Enterprise may wish to see evidence of a current ISO 9000 (quality systems) and ISO 14000 (environmental systems).

Vested interests

Requesters of assurance need to remember that each standard has been developed by a body of self-selected interested parties. In addition, for each standard there exists a commercial ecosystem providing certification, training, and consulting in implementation of the standard. Each standard is owned by an authority, and as such, there exists a commercial interest in the success of that standard, and a need to differentiate the standard from similar standards. In many cases the commercial interest may not be obvious, but without a flow of funds to the standard 'owner', it is not possible to ensure that the standard remains current.

In addition, individual practitioners invest in achievement and maintenance of certification against the standards, creating a vested interest on the part of individuals and organisations that provide standards based or related services.

Internal controls over IT

Therefore COBIT and ITIL, while both providing some comfort that the IT environment of the provider or the Enterprise is well controlled and effectively operating, the standards are different. While there is overlap, there is no commercial interest for the standards owners to either merge or provide a mapping from standard to standard. Each must stand alone, or risk becoming irrelevant and having their commercial space taken over by a competing standard. Add to this the complexity of attempting to map COBIT to COSO (in its various versions).

Auditing standards for external assurance

Auditing standards overlap, and provide the opportunity for confusion or duplication of effort and coverage. In terms of third-party assurance, there is a US standard (the SSAE-16, formerly the SAS70 standard), a Canadian standard (CSAE 3416), and an International standard (ISAE 3402) – all providing generally similar coverage. Similar is important, because each standard starts from a slightly different pedigree and set of objectives.

In particular, the US standards are almost solely focused around financial controls or controls over financial systems, and were born out of the Enron and WorldCom debacles and the coming of Sarbanes-Oxley (SOX) legislation of the early 2000s. This is of limited value if your major concerns are around privately identifiable information. SSAE-16 as a standard is the property of the American Institute of Chartered Public Accountants (AICPA), while the other standards are the property of either the CICA in Canada or the IAASB (International Accounting and Auditing Standards Board).

When requesting such a report from a supplier, the company needs to be aware that the report may not provide any comfort over areas that are of critical importance to the company – product quality, employee safety and building standards, etc. The report will provide comfort that the internal controls over financial reporting (in the case of an SSAE-16) are in place and effective, or the effectiveness of specific controls over access rights, protection of data, or other controls. It is the responsibility of the assurance requestor to confirm that the controls that are subject of the report are controls that are importance to the company purchasing the service or goods.

Sustainability reporting

Vested interests also cover voluntary reporting standards such as the GRI (Global Reporting Initiative), the Global Compact and the SASB (Sustainability Accounting Standards Board). Each has a different audience, different consumers and different drivers for adoption. Yet there remains limited bandwidth within companies to expend resources on sustainability, corporate or social responsibility reporting and action.

Finally there are the competing and overlapping regulatory and legal requirements, ranging from the UK Bribery Act to the US FCPA (Foreign Corrupt Practices Act). Spare a thought for the multi-national Extended Enterprise with a supply chain that must be able to demonstrate compliance with the plethora of regulations.

A small sample of standards

Each standard shown in table 11.1 requires an infrastructure of support, to develop and maintain the standard, to communicate the standard, and an ecosystem of practitioners who can implement or certify compliance with the standard. Thus the development, promulgation, communication and maintenance of standards is expensive, and requires a demonstrable return to those responsible for the standard.

Table 11.1: A small sample of standards

• COSO ('92, ERM, 2013) - Internal Controls	• BS 11000:2010 - collaborative business relationships
• SSAE-16 (former SAS-70) - Internal Controls	• CiPFA - RM Across Shared Services Lifecycle
• ISAE 3402	• AA1000AS
• ISO 27001 - Information Security	• Codes of practice
• BSI 25999 - DRP/BCP	• BS 8903:2010 - Procuring Sustainably
• ISO 9000 series - Quality systems	• ITIL - Information Technology Infrastructure Library
• ISO 14000 series - Environmental systems	• COBIT - Control Objectives for IT
• ISO 31000 (and others) - RIsk Management	• SA8000 - Socially Acceptable Practices in the Workplace

Reporting Standards

• GRI (global reporting initiative)	• IIRC
• IFRS/GAAP	• SASB
• Global Compact	

Regulation and Legislation

• UK Bribery Act	• FCPA
• Solvency II	• FATCA
• Basel II	• Basel III
• Basel IV?	

Jurisdictions:

When looking at the range of standards, there is the added problem of jurisdictions, as some standards are "global" while others are national or regional in nature. For example, the SSAE16 (formerly SAS-70) is an assurance standard for service organisation, and is applicable to US businesses, while the CSAE 3416 standard is applicable to Canadian businesses, and the ISAE 3402 standard is applicable internationally.

An international or multi-national extended enterprise may have difficulty in determining the appropriate standard(s) to accept or require from suppliers. Equally, the provider of services could, depending on the geographical spread of its existing clients, balanced against potential target markets, have a similar difficulty in understanding what standard(s) they should be demonstrating compliance with.

Death by gap analysis:

With so many standards, could a company simply select a minimal set of standards, and then require suppliers (or customers) to accept those standards, or to provide a gap analysis to show how the 3rd party used standards vary from the accepted standards? While this may seem to provide an elegant and simple solution, the problem is that such a solution requires a deep knowledge of potential standards on the part of all involved.

Any gap analysis begins with the assumption that the reviewer knows at least two standards in detail -the "accepted standard" and the alternative standard in use by the third party. There is then the performance of the gap analysis itself, and the determination of the importance and acceptability of the gaps identified.

In the end, reliance on a single set of standards coupled with a gap analysis on a case by case basis will result in

excessive resources being used simply in the mapping of standards and negotiating acceptable deviations from the accepted standards.

Cascading standards trap:

A further problem with the plethora of standards is the danger of cascading acceptance of standards because the standards "cover generally similar areas". Would any company accept the UN Global Compact as an adequate set of standards for assurance? Yet, it is not difficult to cascade from almost any standard through to the UN Global Compact standard.

For example, we could begin with a requirement for an ISAE 3402 report. From there, we will accept (as being similar and partially overlapping) ISO 90001 compliance (the quality standard that requires documentation of processes), and from there to accepting an ISO 31000 (Risk Management standard), and from there the next supplier in the chain says they can provide an ISO 14000 certification (environmental systems) instead, with the next supplier having a GRI (Global Reporting Initiative) report, which after all, is simply a longer version of a UN Global Compact report (not true, but for the sake of the argument). While the above example is silly, and intentionally so, it serves to point out that danger of cascading standards acceptance.

Single standard variance:

Even with the acceptance of a single standard, there remains the question of the multi-supplier cascading of application of that standard. In this case we can consider ISO 27000, information security. While the enterprise may require ISO 27000 certification of suppliers, what confidence is there that the certification, multiple steps away from the core enterprise, actually covers the aspects of the suppliers' business systems that support the core enterprise's business?

Therefore, it could be possible that the assurance being provided via certification does not actually cover the systems, processes or data that are within scope of the relationship.

Desired outcomes from assurance

The provision of assurance has always been a kind of game in which one party agrees to deliver an opinion that will give management comfort, at a cost that the requestor of assurance is willing to pay. This conflict, how much assurance can be provided balanced against the risk associated with that assurance at the agreeable price, represents a key limitation on the level of assurance that can actually be delivered.

The objective is to reach a level of balance in which the assurance provider limits the risk that they carry, and in exchange the assurance requestor determines that the level provided will be adequate. Of course, the more the requestor is willing to pay for assurance, the greater the level of depth, quantity of testing, and in some cases quality of people, that the assurance provider will be able to apply. Both parties (provider and requestor) have desired outcomes from the assurance process. Here, however, we will focus on the requestor or purchaser of assurance. The following is a short list of what we might expect an Enterprise to seek for assurance:

- Comfort
- Evidence
- Compliance
- Trust
- Shared risk

Comfort

Fundamentally the assurance requestor wants to know that they do not need to worry. Worry is brought about in large part by the gaps in our knowledge coupled with the potential negative consequences arising from something slipping through the gaps in knowledge. The unknown supplier multiple steps away employing child labour, or the insecure information system holding personal information about employees.

Evidence

By themselves statements from a supplier hold limited weight and need to be backed up by evidence. One form of evidence is an assurance report produced for the supplier either on their own activities and processes, or on the activities and processes of their downstream suppliers. Of course, this begins to highlight an issue with the assurance model - assurance is only as strong as the weakest performed assurance through the supply chain. One supplier unwilling to pay for effective assurance and a report produced based on inadequate investigation or assessment, and the entire trail of assurance collapses.

Compliance

Demonstration of compliance with standards (through independent certification) or regulation.

Trust

The assurance requestor wants to feel like they can trust the supplier. Sometimes this comes through personal contacts and social relationships, but as soon as the Enterprise is "extended", and in this case we would suggest beyond a simple procure/provide model with no additional steps or degrees, then trust must become institutionally based. For example, international letters of credit provide the basis for business activity via the trusted intermediary of an international bank.

Shared risk

Finally there needs to be an understanding that risk is being shared across the supply chain, and that all participants contribute to achievement of other supply chain participants' objectives. Where it is clear, or suspected, that one party's objectives can only be achieved should another party fail, then too many share in the risk of the failing party. That results in a need to understand where objectives are out of alignment and thus where shared risk can transform into our risk.

Who provides "assurance"?

Now that we have considered the need for assurance, the various standards and their conflicting interests, we need to consider who provides assurance. Is this something that can only be provided by an external party, or can internal resources provide assurance, and if so, who within the company can provide assurance?

Management and the three lines of defence

There is currently a fixation with the "Three Lines of Defence" (TLD) model of internal control, in which management provides the first line of defence, risk management or similar oversight/compliance functions the second, and Internal Audit or other independent sources of assurance the third.

On the one hand the model provides a simple and clear segregation of responsibilities. Each element has clearly defined remits, and the overlapping levels of control and review should ensure that risks and control weaknesses are identified early and resolved. On the other hand, an attempt to rigidly implement the Three Lines model can lead to the silo-isation of internal control and risk management, undermining the ability and willingness of management and oversights functions from raising issues with each other, and accepting recommendations.

From an Extended Enterprise perspective, the TLD model can introduce a level of ambiguity in terms of responsibility for the performance of vendor assessments or other processes for the achievement of assurance throughout the extended enterprise. Who is responsible within the enterprise to ensure that stakeholders, both upstream and downstream (not to mention on both banks of the stream) are providing or receiving the assurance that they need?

Management certainly must provide internal assurance of effectiveness of controls and operations. That can include ensuring effective assurance is being provided to customers, and demanding appropriate assurance from suppliers.

Yet Risk Management frequently is the part of the organisation tasked with actually performing the assurance review (or vendor assessments), and providing certification to third parties.

What is the role of Internal Audit? Perhaps to review the effectiveness and completeness of such vendor reviews? Liaise with external parties to confirm that they are received the levels of assurance that they require? This is not in the traditional mandate of Internal Audit, and simply is not (or rarely) performed by that function.

Independent?

What are the ranges of assurance that would be desirable, if assurance is desired? How 'deep' into the extended environment can assurance be reasonably achieved / afforded?

- Internal (?)
- Certification
- Attestation
- Review

Are assurance standards and certification standards capable of providing assurance or even a level of comfort that the assurance provided is meaningful?

Requestor

When looking at assurance through the eyes of the requestor of assurance, there are four factors that need to be considered:

- What are we seeking assurance over?

- Who is the audience of this assurance
- What is the cost of assurance?

Earlier we explored why Enterprises seek assurance, but to reiterate, the primary purpose is to provide management (and through management, stakeholders) with comfort and confidence that all parties will meet their agreed deliverables and obligations.

What?

A first question has to be; what is the scope of coverage of the assurance provided, and what is the validity of that coverage? Companies can and do seek assurance covering a range of business activities, and such assurance needs to be appropriate to the specific areas of risk that represent the greatest area of concern for the purchaser (and seller).

Where a service provider manages or holds personally identifiable information on the employees or clients of the purchasing company, it is important that the provider be able to demonstrate effective controls over access to that data, protection of that data, and processes to identify breaches of security over the data.

Assurances also need to be to an appropriate depth within the supply chain. A recent internal study by Zurich Insurance showed that personal information for automobile accident claims were shared with up to 21 entities for various insurance claims management purposes.

Mending the assurance model

Given the imperfections of the current situation how can we best improve things in both the short and longer terms? The key short term action needed is that the Enterprise must select the assurance standard that is most appropriate to their specific needs, and require their suppliers to demonstrate compliance in a consistent and co-ordinated manner. This will mean that providers of this assurance will almost certainly need to shoehorn their responses, supporting evidence and even certification into the requesting company's preferred standard. Equally this means that the enterprise will need to be aware that their customers may require them to do the same, i.e. comply with a different standard than their preferred option, or indeed not the standard that they have paid to be certified as being compliant with.

A number of circumstances will need particular consideration:

- The length of the enterprise's supply chain – how many levels does it have and how effectively can each tier control the tier below?
- What is the geographical nature of the enterprise and what are the potential jurisdictional conflicts?
- Is the enterprise operating in a shared services environment (either as customer or supplier)?
- What IT/Cloud environment is the enterprise working within?
- Does the enterprise need assurance at the line item level and how can this be delivered?
- Is the enterprise operating in a regulatory environment?

The objective is to reach a level of balance in which the assurance requestor determines that the level of assurance provided will be adequate to address their risk profile and understands how the assurance provider will wish to limit the risks that they carry in exchange. In arriving at the decision on which assurance standard to select we therefore propose that enterprises ask a number of key questions in addition to the environmental questions above:

- What risks are we seeking assurance over?
- What risk exposures are the assurance options valid for and which best meets our circumstances?
- Who can most effectively deliver the assurance we need?
- How much will the assurance we need cost and can we and/or our suppliers bear it?
- What period do we need assurance over? For example:
  - Is a 3-year window adequate?
  - Is a 10-year window adequate?
- Are we operating in a regulatory environment and what will our regulators expect (or indeed be able to provide)?
- What will our stakeholders and society at large expect?
- How can we include our requirements in our contracts and ensure we have a right to audit, which we have the capability to undertake effectively?
- How can we monitor delivery of the required assurance in our day to day contract management?

A future assurance model?

As for fixing the overall assurance model for the future we need to consider more radical options, as a number of the issues we have raised have multi company, multi supplier and often industry/sector wide implications, which are beyond the power of most enterprises to resolve independently.

To address this we advocate consideration of establishing Assurance Clearing Houses by industry, in which the clearing house performs the assurance and all providers / suppliers throughout the extended enterprises within that industry need to be able to demonstrate that they are members of and have been certified to the requirements of that clearing house. The key to achieving this would be industry agreement to and joint funding of such clearing houses.

Development of such industry based Assurance Clearing Houses would require a number of key parties in any industry to collaborate and fund the initial establishment of such an assurance body. In addition, the cost of compliance would need to be accepted as a cost of business and all parties in the supply chain would need to understand that the cost of compliance would flow through the system. On a practical level, this may require some major players in any industry to contribute a higher overall percentage of the cost of the Clearing House.

Likewise, participants in the supply chain will find it advantageous to be able to demonstrate both participation in and certification by the industry Assurance Clearing House. Further cost saving will be achieved by requiring suppliers to gain a single assurance certification and not multiple certifications, based on their customers' individuals assurance standards and requirements.

Summary

Fundamentally, assurance is the process to help executives and stakeholders sleep at night. In this chapter we have explored the role of standards in assurance models, focusing on the difficulties posed by having to deal with multiple overlapping, potentially conflicting, incompatible, costly and collectively inadequate standards.

As we have outlined, the ability to receive and provide assurance is undermined by the wide range of standards for assurance and the selection of standards (applicable to that business) by each participant in the Extended Enterprise. In addition, each standard represents a vested interest and covers only a defined subset of business processes and systems and therefore provides limited coverage, which is not always aligned with actual risk profiles. To achieve complete coverage, multiple standards can be required.

As the key objective is to achieve a level of balance in which the assurance requestor determines that the level of assurance provided will be adequate to address their risk profile and understands how the assurance provider will wish to limit the risks that they carry in exchange, we have suggested a number of factors to consider and questions for enterprises to ask. A number of these are explored in more detail in other in this document.

Further information

Further information about auditing shared and outsourced services can be obtained from the Institute of Internal Audit:

http://www.iia.org.uk/buy-iia-technical-guidance/

Chapter 12: Supplier assurance - advancing from assessment to risk management

Richard Hibbert, Surecloud

Organisations are facing an increasing need to introduce supplier assurance programmes in order to reduce the risks associated with essential supplier relationships. Existing approaches tend to focus on the audit process and are heavily biased towards supplier questionnaires, taking a one size fits all approach. As 21st century businesses extend their supply chains to better compete in the global marketplace, is now the time to look at a more considered risk centric approach to supplier assurance?

Why is supplier assurance necessary?

The notion and practice of gaining competitive advantage by leveraging supply chains is not new to modern business – nor is the maxim "an organisation is only as strong as its weakest link", or supplier in this instance. However, business has changed dramatically over the last 15 years with the advent of the Internet. Thanks to the World Wide Web, business can now be conducted at the speed of light, for example suppliers can be sourced electronically from any part of the globe, without any face-to-face contact; information can be exchanged at the click of a mouse; and commercial transactions can be concluded in seconds.

As digital trading relationships have evolved, the boundaries between organisations have eroded making them difficult to define. The new wave of cloud suppliers and IT-as-a-service has led to a flurry of business process and service outsourcing, further exacerbating the situation. Consequently, organisational perimeters have become blurred. Many relationships are built on trust, and this becomes diluted as relationships proliferate along the supply chain. A more rigorous level of assurance is needed for organisations to be sure that their suppliers, and their suppliers' suppliers, are meeting the same commercial and legal requirements that they are. Suppliers have an obligation to meet an organisation's requirements, but ultimately the accountability for ensuring all contractual and regulatory requirements are met lies firmly with the organisation.

Whilst a wave of compliance guidelines and requirements (including FCA SYSC 8.1, PCI DSS, ISO27001, EU cyber security directive, ICO legislation for information security) has led to an increase in auditing activity in some circles (where it almost appears like everyone is auditing everyone), a significant number of organisations are still failing to obtain assurance regarding their suppliers' security standards. For instance, in a recent survey of 172 organisations[12], only 65% of respondents ensured that the contract with its externally hosted service provider included provisions for security.

It is perhaps difficult to understand why this percentage is not any higher, especially when you consider the consequences of getting it wrong. The recent horsemeat scandal is a good example of how failure to properly check suppliers' credentials and processes led to widespread food fraud. The global retailers and food companies with multi-level supply chains suffered considerable brand damage and lost revenue as a result, and still face the potential of fines and criminal proceedings.

What supplier risks should we be concerned about?

Supplier relationships can yield significant benefits such as providing economies of scale or introducing new capabilities. However, they also have the potential to introduce significant risks to an organisation's operations, particularly if the supplier is unqualified, has not established robust internal processes, or does not follow industry standards.

We should also consider that different suppliers potentially expose organisations to different levels of risk; an outsourcing partner providing process support is more likely to expose an organisation to higher risk than a company that has a purchasing contract to supply stationery.

Source: 2013 Information Security Breaches Survey, Department of Business Innovation & Skills in conjunction with PwC

In order to understand the risk to which a supplier may expose an organisation, it is useful to understand the broad categories of risk as follows:

- Strategic – the supplier's goals may conflict with the organisation's goals, for example a change in product direction, or focus on a strategic relationship with a competitor;
- Operational – a failure of technology, inadequate staff vetting policies, loss of key people or insufficient financial resources can result in the supplier not meeting their contractual obligations;
- Regulatory and legal – the supplier has inadequate compliance systems and controls, or the contract proves inadequate as a means of ensuring the supplier meets its obligations such as service levels, or the right to audit;
- Reputational – a poor service from the supplier, or unauthorised disclosure of confidential information, can lead to the organisation being perceived in a negative light, leading to brand damage and loss in customer confidence and loyalty.

When designing a supplier assurance programme it often helps to identify the categories of risk for each supplier, so that assessments are not unduly onerous, or conversely, lack the detail to effectively assess a supplier's current situation.

What challenges does supplier assurance pose?

Historically, small teams of people have had the challenge of managing internal risk and compliance programmes. Introducing the need to audit suppliers therefore multiplies the compliance activity by the number of suppliers, in a fairly linear fashion. Each new supplier incrementally adds to the effort, with little or no economy of scale.

Typically, self-assessment questionnaires are used to determine each supplier's conformance with the organisations desired requirements. In the absence of application software, spreadsheets containing the questionnaires are emailed to suppliers to complete and return. Whilst they are a convenient tool to record information about a supplier, they do not scale well, even for a handful of suppliers. Collating the data is difficult to manage, as is version control. Relying on email to distribute the requests to suppliers provides no information about how suppliers are progressing, and about how good their responses are. Further, any analysis that has been built into the spreadsheet is difficult to aggregate, hence providing a meaningful comparison of suppliers is difficult.

Establishing a supplier assurance programme

As you can imagine, supplier assurance programmes are extremely labour intensive – for both the organisation and its suppliers. Earlier we touched on the use of mechanisms such as spreadsheets and email to distribute assessments. Tracking and managing the progress of each assessment involves lots of email and telephone calls; there is little visibility across the programme with such an approach. This is even before considering tracking remediation of non-conformities.

It is therefore not in anyone's interest to over-complicate the assessment process. Central to this concept is understanding each "type" or category of supplier in terms of their products and services, the relevancy of each requirement, and the impact on operations if the service fails. By taking these factors into consideration, and by grouping suppliers accordingly, we avoid the "one size fits all" trap, which often leads to unsuccessful assurance programmes. For instance, where risk ratings are acceptable and where evidence of compliance is provided, shortcuts can be given to allow the supplier to bypass questions that are superfluous.

As well as understanding the risk associated with the "type" of supplier, we must also consider risk in terms of the information that is stored, processed or transmitted by the supplier. Unauthorised disclosure of confidential information, can lead to breaches in contract and/or data privacy laws, the latter often leading to significant public exposure, reputational damage and fines.

By understanding the various categories of supplier and information risk, we are able to decide whether or not more than one variation of the questionnaire should be designed into the supplier assurance programme; for small programmes it may be overkill.

Another aspect to consider is the use of a phased risk-based approach to auditing. For example, an organisation with the primary concern of maintaining data privacy across the supply chain may choose to phase the risk assessment process in the manner detailed below:

Phase 1: Information classification – define your objectives (based on your auditing requirements) and

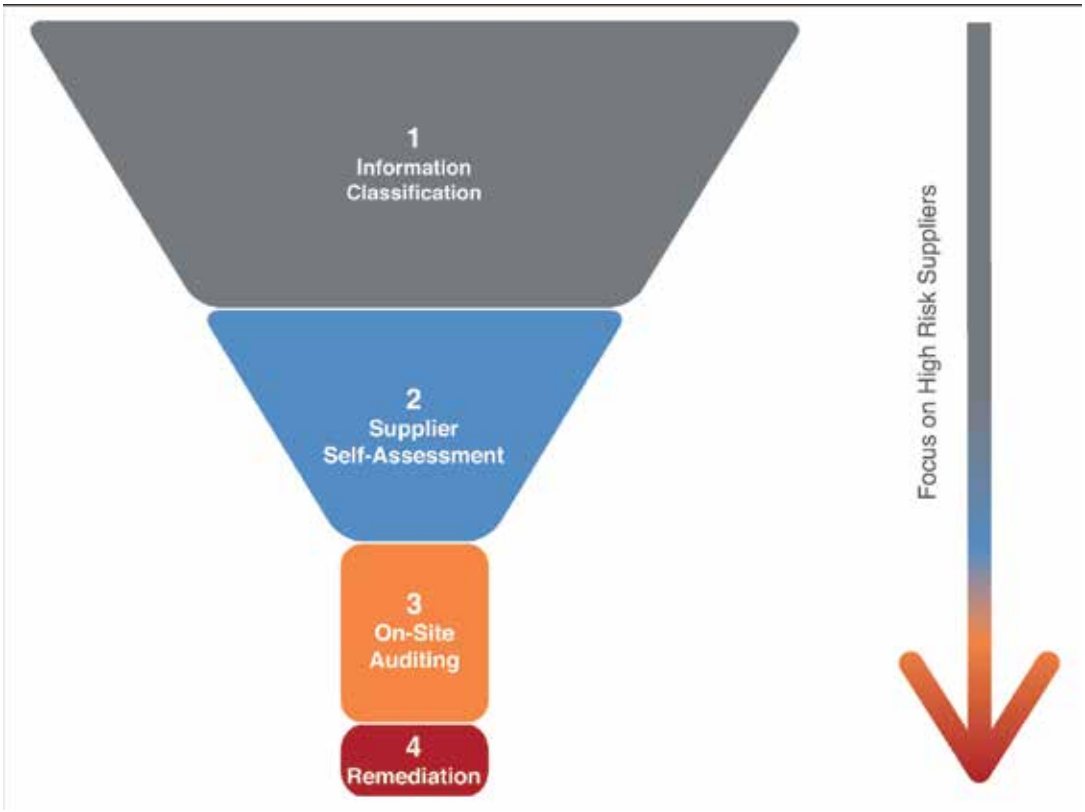


Figure 12.1: Supplier risk assessment

decide what information is most critical, (e.g. name, address, contact details, bank account number, credit card number etc.).

Define a Supplier Risk Rating based on the type and volume of information – e.g. ratings might be Low, Medium, High and Critical. Assess all suppliers with the information classification questions, and generate a Risk Rating for each. The Risk Rating can be used to prioritise which suppliers move to phase 2 as a priority. This approach in effect gives an organisation the ability to audit all suppliers quickly and produce a risk register; a rank ordered list of suppliers by data risk.

Phase 2: Supplier self-assessment – formulate your questions carefully, avoiding ambiguity and repetition. Qualitative questions should be given a weighting according to importance, to enable risk to be calculated, i.e. 1=low, 2=medium, 3=high, 4=critical. Hide your measurements to avoid making the "correct" answer obvious. Consider risk from a strategic, operational, regulatory, legal and reputational perspective as discussed earlier and formulate your questions with these in mind. Ensure you coordinate with all other departments requiring information from suppliers. Give your suppliers access to online forms into which they can enter the information you need. You should be able to check on their progress as they complete the questionnaire – see automated supplier assurance below. Once the information has been submitted, supplier risk can be calculated automatically; aggregating the information will enable suppliers to be ranked according to risk, based on the weightings applied to the questions. Again the risk scores can be used to prioritise supplier for the next phase, to ensure supplier's posing the greatest risk are audited first. Even for organisations with a small number of suppliers, e.g. five or more, an automated approach will drive efficiency.

Phase 3: On-site auditing – in-person supplier audits should be undertaken to validate the information supplied. You may not need to visit all your suppliers, so you can prioritise visits based on the highest risk suppliers from Phase 2. This will enable you to utilise your compliance resources as efficiently as possible, save time, and shorten supplier assurance cycles.

Phase 4: Remediation of high-risk suppliers – based on the findings of the on-site visits, suppliers can undertake tasks and projects to improve their risk scores. These

should be recorded online to enable you to check on progress, repeat phases 1-3 where necessary, and to make more informed risk-based decisions about whether to maintain supplier relationships.

What can an automated supplier assurance programme deliver?

Small supplier assurance programmes can be managed using office productivity tools, however there is a critical point where such an approach will deliver diminishing returns; administration of spreadsheets becomes the primary activity, rather than assessing risk and using this to drive improvements in supply chain compliance.

An appropriate automated solution could include the following features:

- Internet enabled - providing centralised access to each self-assessment questionnaire would reduce administration as spreadsheets would no longer be distributed via email. Risk teams would have instant visibility of questionnaire progress;
- Evidence library - allowing suppliers to upload documents to provide evidence, such as policy documents or certificates of compliance. The library represents a single location where all evidence is stored and documented and therefore such documents are no longer sent over email;
- Granular permissions - for example, hide fields (such as scores) that are only relevant to the auditor, and control which questions are visible during each phase of a multi phased programme;
- Integrated task management, messaging and workflow - enabling the efficient management of the supplier, the self-assessment and subsequent remediation phase;
- Alerts - notifying the organisation when Tasks become overdue or certificates in the evidence library are due to expire helps towards maintaining continual compliance; and
- Centralised dashboards - providing real-time visibility of the compliance process with key risk indicators and reporting to support the operational needs of the auditors and the decision making needs of the business.

Automation does require financial investment, but economic buyers need to consider that as organisations reap the benefits associated with "extending" the enterprise, these do not come without risk. Organisations need to develop new capabilities to deal with the increased levels of risk, and automation is key to delivering these capabilities.

What other considerations are there when implementing a supplier assurance programme?

Contracts

Ensure supplier contracts include a provision giving you the right to audit the client; some suppliers may be short-sighted enough to refuse, at which point you have little recourse other than to see the contract out or find an alternative supplier willing to cooperate.

It's is also a good idea to stipulate the timeframe for addressing any non-conformances. This may be based on severity of the requirement e.g. Major – 2 weeks; Minor 4 weeks.

Asset register

It is extremely useful to get the supplier to specify which of their assets store, process or transmit your information (including third party suppliers of theirs). Performing such an exercise will prove the supplier is in control of your data.

Consolidate your organisation's audits

Some suppliers aren't receptive to different audit questionnaires from different sources within the same organisation, so work with other departments to consolidate your company audits into one. This requires some upfront effort but will ultimately reduce repetition and streamline the process, reducing the total supplier man hours spent responding to your organisation. In addition, it will ensure that should you need to undertake an on-site audit, you won't exceed your audit allowance.

Set expectations and book your slot

Suppliers need to allocate time and resource to complete audits so communicate your timelines in advance so the audit doesn't come as a surprise. This is also a good time to explain the scope of the audit so that the supplier can assign responsibilities to different team members and also ensure that key requirements are in place before the audit is received.

Summary

The benefits of supplier relationships are immediately obvious, however organisations need to ensure that they fully understand and control the associated risks. The volume and ephemeral nature of supplier relationships ultimately calls for assurance capabilities that are structured (consistent and repeatable), agile and efficient, so that they can be embedded in operational processes – becoming part of the DNA of an organisation.

Automation is key to delivering such capabilities, and although this means incurring costs, it also creates value: reducing risks in operational activities and providing the structure and efficiencies that are key to controlled business growth whilst maintaining high levels of quality. The case study below illustrates how a large online retailer used automation to improve its supplier assurance capabilities, readying itself for the demands of the 21st century extended enterprise.

Case study:

Shop Direct

Shop Direct, a £1.7 billion online retailer with 800 suppliers, needed to automate its spreadsheet-driven supplier assurance programme. Suppliers were asked to complete a questionnaire held in a spreadsheet and return it via email. Then, they were visited by the compliance team, in order to validate the information received, and establish further actions. Being manual, this process was incredibly time-consuming and unwieldy, as managing multiple spreadsheets is a notoriously complex challenge. Hundreds of emails were exchanged between the team and suppliers. Version control of the spreadsheets was a headache, and auditing the predominantly qualitative information relied heavily on the experience of the team rather than on analytical evidence. In addition, collating and aggregating the information in order to rank and compare suppliers was virtually impossible. Much of the work undertaken was administrative, chasing suppliers by email and telephone to return their spreadsheets, which meant that the team's auditing skills were not being effectively utilised.

SureCloud worked closely with Shop Direct to deliver its new centrally-managed and automated third party assurance programme. The questionnaire was re-designed to avoid ambiguity and repetition, but most importantly to gain quantitative (rather than qualitative) information wherever possible, in order to facilitate vendor risk analysis. The questionnaires were made available to suppliers through a cloud-based platform, giving Shop Direct instant visibility of Questionnaire completion and risk metrics across the entire programme. Centralised task management and workflow allows Shop Direct to manage suppliers through each assessment phase, and is particularly important when prioritising, allocating and tracking remediation activity. This has delivered the following benefits to the retailer:

- Simplified the third-party assurance programme;
- Delivered an instant view of compliance status across all 800 suppliers;
- Enabled informed decision making based on risk dashboards;
- Eliminated the pains associated with manipulating spreadsheets;
- Generated time savings of at least 0.75 FTE by reducing administrative workload;
- Provided faster and easier interface for suppliers to use;
- Contributes to improved customer service and brand protection.

"The auditing team of three was each spending 25% of their time on the administrative tasks required by our manual processes. Our use of the automated SureCloud platform has given us this time back, so we can focus more heavily on data analysis to establish more reliable risk assessments, to add value to our business."

"SureCloud's real-time dashboard provides an instant view of where we are with data compliance. The responses given by our partners will determine which suppliers we should focus more on. And with a few clicks, we can produce reports such as our ten most high risk suppliers."

Chris McAteer, Director of Compliance and Operational Risk at Shop Direct Group

Chapter 13: IT and cloud computing

Darren Brooks, Daniel Roberts, Depeche Elliot

Introduction

Advances in workplace technology and more specifically information technology have driven significant change in enterprises since the 1980s. This change has enabled new modes of communication and interaction with colleagues, collaborators and customers. It has also enabled new business models where: enterprises can have a storefront in every home, but none on the high street; IT applications and data processing can be provided in the cloud, sharing expensive infrastructure and development costs; or tasks can be outsourced to low-cost locations many thousands of miles away. The extension of the enterprise is largely driven by the enabling factor of the new information and communication technologies. However, the increasing reliance on information and communications technologies by enterprises has introduced new risks to their revenue streams that must be understood, considered and managed. This chapter will consider the risks facing the extended enterprise from its use of technology and will identify some potential mitigation measures that can be introduced to manage those risks.

Technology in the enterprise

Technology risk

Information technology risks manifest from threats that can be divided broadly into adversarial and non-adversarial threats[15]. Adversarial threats are the deliberate actions of a third party intent on interacting with the enterprise IT systems in a manner that causes the enterprise disruption or loss. Examples of adversarial threats include:

- Perform reconnaissance and gather information about the enterprise IT network.
- Craft or create attack tools such as phishing attacks or spoof websites.
- Deliver/insert/install malicious capabilities. Insert malware onto target systems on the enterprise IT estate.
- Exploit and compromise vulnerabilities to achieve the aims of an attack.
- Conduct an attack e.g. communications interception, denial of service attacks, physical attacks or social engineering attacks.
- Achieve results e.g. steal sensitive information, destroy data or physical systems, modify or corrupt data.
- Kidnap or manipulation of employees or their families to gain privileged access to systems.

Non-adversarial threats manifest as events that are either examples of human error, environmental events, or component failures. Examples of non-adversarial threat events include:

- Accidental data loss e.g. lost laptop, disk, or memory stick.
- Incorrect settings enabling accidental access to sensitive or private information.
- Fire / flood / earthquake / tornado at primary or backup data centre.
- Disk failures or fundamental system design flaws.
- Electrical supply interruptions

IT risk management using technology solutions

A technological risk management solution will be subject to the same failings and requirements noted in the previous section. The solution will be reliant on the quality of the data entered by people using it to manage risk and will not be able to magically improve that data quality or make significant management decisions on risk by itself.

A good IT risk management solution will: remove duplication in the process; improve collaboration between stakeholders, enable real time assessment and monitoring of risk, enable threat intelligence sharing and establish a common risk taxonomy. A good solution

15. NIST Guide for Conducting Risk Assessments (800-30 Sept 2012)

will also provide data integrity, enable segregation of duties and provide an audit trail of risk decision making.

In other words good technology should free up users to focus on risk management, mitigation and remediation.

Technology as an enabler

The modern extended enterprise environment demands the use of technology to facilitate risk management. A robust risk management programme that traverses the enterprise and includes all external stakeholders needs to leverage technology in order to provide the level of attestation required by policies and regulations.

Technology solutions do not in themselves provide a "silver bullet" to solve all the enterprises' problems, however, a combination of good technology; strong risk management framework and people with the right skill set and training can ultimately provide adequate levels of security for the enterprise.

Poorly managed risk and compliance generates complexity, redundancy, and failure. Too often organisations are reactive and lack a cohesive strategy. This isolated and periodic snap-shot approach to risk and compliance causes organizations to spend excessively on internal management and external auditors.

Technology helps tie together and unify the extended enterprise providing visibility and access to data, enabling the business to act in a timely and consistent manner.

Mobility/BYOD/WOAD

Mobility

Enterprises have been providing mobile telecommunications devices for employees for over thirty years. The introduction of IP based technologies on the mobile networks has encouraged the development of a range of mobile devices which have taken enterprise data and applications beyond the corporate property boundaries. Mobility solutions introduce risk to the enterprise because it no longer has physical control over access to the end point device and because data on the device can be intercepted at rest and in transit. Mobile devices are also difficult to manage because they encompass a range of manufacturers and different operating systems and also because the technology changes very rapidly. Consumer mobile devices have evolved over the last five years to the point that they are often more powerful and easy to use than the device issued by an enterprise which leads employees to demand the same level of service at work or to be able to use their own devices.

Consumerisation

Consumerisation is a trend towards IT innovation being driven in the home and influencing enterprise IT development. There have been numerous examples like the rise of the tablet and the success of IPhone where employees have grown used to ways of accessing information and then demand similar capability in the workplace. Many organisations now offer an employee app stores for Android or IOS rather than use browsers for access to enterprise data and applications. The risk for enterprises is that in trying to keep pace with employee demands they are missing opportunities to innovate in a different direction.

Bring Your Own Device (BYOD)

Bring your own device (BYOD) is the concept of allowing employees to access corporate email and other applications and data via their own smartphones, personal computers, and tablets. BYOD is often popular with employees as it means they only need to carry one device. It can also be potentially cost effective for the enterprise if managed well. There are risks for the enterprise in allowing BYOD: employee's devices are harder to control and manage; the device may act as an infection vector for malware into the enterprise; an enterprise may not be able to remove data from the device; there are privacy issues that must be managed where controls are introduced on employee devices; enterprises need to be aware that personal data will exist on the employees device and must consider the potential impact of any device wiping policies. There is a need for robust policies that are continuously maintained and clearly communicated to the employees.

Work On Any Device (WOAD)

Work on any device (WOAD) is an extension of the BYOD concept which allows employees to access corporate email and other applications and data from any device in any location. WOAD increases employee flexibility, but it usually also requires the enterprise to relinquish control over the end device. Most of the risks associated with mobility and BYOD apply to WOAD, with an increased risk of the employee accessing the corporate data and applications from a device infected with malware.

Cloud services

Types of cloud services

Wikipedia provides a definition of cloud services as "the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet)". The growth of cloud services has helped enterprises from small to large to manage their IT estates more effectively. Small enterprises can make use of access to processing capabilities with levels of resilience that would be beyond their means to build internally. Large enterprises can potentially make cost savings from outsourcing some or all of their IT estate. Small enterprises can potentially gain access to applications that would previously have been beyond their means to buy or develop.

Cloud computing is offered in four types:

Public – a shared infrastructure made available to all by a service provider across the internet. The risks associated with using Public cloud include security risks due to their relatively open nature, availability risks as SLAs tend to be weaker than can be contractually agreed in private clouds and the risk of legislative compliance breaches as data crosses national borders.

Private – the cloud infrastructure is dedicated to a single enterprise customer. Private cloud is generally less risky than the alternatives, although the supplier failure risk is higher as the enterprise is more dependent on the cloud provider.

Community – the cloud infrastructure that is shared among several enterprises that manage and secure the cloud for their mutual benefit. This cloud type generally has a lower security risk than a public cloud as the tenant enterprises can better manage security risks. The supplier failure risk could be higher than a private cloud as the supplier could be impacted by the loss of a significant tenant.

Hybrid – is a collection of two or more cloud types (private, community, or public) where the enterprise requires the advantages of a private or community cloud while taking advantage of public cloud services to augment capacity or offer a specific software service. A hybrid cloud is likely to present the greatest security risk as data and applications must be maintained across different boundaries and potentially with multiple suppliers.

The types of services offered in the cloud include:

Infrastructure as a Service (IaaS) – is the most basic cloud service where either physical systems or more usually virtual machines are provided with an agreed set of service levels. The solution can potentially scale to meet with user demand at different times without the customer needing to own and operate the infrastructure required to deliver the full service level. The cloud service provider's business model enables them to share the infrastructure between customers that have different levels of demand at different times and to achieve economies of scale. The key risks to this service include: potential outages to system, power, or environmental failures; security risk as a result of access control failures, privilege escalation or vulnerabilities in the underlying infrastructure; or business risk due to the failure of the service provider.

Platform as a Service (PaaS) – is a cloud model where the provider delivers a computing platform that usually includes operating system, programming language execution environment, database, and web server. The key risks to this service type are much the same as those for IaaS, although it is more straightforward to achieve security segregation for PaaS than IaaS.

Software as a Service (SaaS) – is a cloud computing service model that provides access to application software and databases that are hosted centrally and accessed via a web-browser.. The risk profile is broadly similar to IaaS, except that the risk of attackers being able to gain access to the underlying systems should be lower. In fact, some SaaS implementations (Salesforce.com for example) are generally considered to be more secure and reliable than in-house CRM solutions.

Network as a Service (NaaS) – offers a cost effective way of using shared network infrastructure to connect enterprise networks to the Internet and cloud services to provide flexible and extended VPN and bandwidth on demand. NaaS offers an enterprise a compromise in terms of risk between the lack of security and availability risks associated with the Internet and the cost of dedicated network infrastructure.

Common risks associated with cloud services

Geographic risks – cloud service providers can move data and applications to any of their geographic locations unless prevented by service level agreements. This could potentially mean that Data Protection or other legislation is breached.

Cultural risks – cloud solutions can cause "political" difficulties within enterprises that have not been active outsourcers, also some cloud solutions or providers may not be well suited to working with the enterprise.

Technical risks – does the cloud solution match the enterprise's service requirements precisely and will it integrate with existing infrastructure or systems?

Availability – the key benefit of a cloud based solution should be management of business continuity and disaster recovery. However there is a risk that the provider's plans may not meet the enterprise's recovery time and stated requirements and that other key customers may be given priority for recovery in the event of any catastrophic disaster. Furthermore, placing key applications with cloud service providers introduces the risk of supplier failure impacting the enterprise's operations. The enterprise should have a clear recovery plan in the event of the loss of service due to supplier failure.

Legal risks – the enterprise needs to be sure that the cloud provider can meet all the required legal, contractual and moral obligations. Legal risks cannot be transferred and the enterprise will usually be held responsible for any legislative breaches that occur at a cloud provider. One of the key risks to address is compliance with data retention requirements and ensuring the destruction of data at the end of its life.

Supply chain risk – The increasing use of cloud solutions in the extended enterprise may result in suppliers placing enterprise data in the cloud without the knowledge or permission of the enterprise. Supply chain assessments should review this risk regularly and supplier contracts should state whether the enterprise accepts cloud-based processing of its data.

It is important to understand that whilst a good service level agreement combined with a robust Cloud Service provider assessment will help mitigate most of the above risks, the legal risk remains with the organisation and needs to be carefully managed.

Risk responses

Governance culture

Decision making and delegation at CXO level.

The board of an enterprise must take responsibility for managing IT and Cloud risk. The management team needs to ensure that an appropriate person is given responsibility for owning, reporting and managing IT and Cloud risk. This person needs to be able to explain the risks to the board so that they are able to provide strategic direction, choose which elements to delegate and take key risk management decisions.

A recent paper from the Institute of Chartered Secretaries and Administrators[16] provided a number of points for a board to consider:

- Understand your company's cyber risk. It is very specific to an individual organisation's situation, even within a single market sector.
- Make an active decision as to the balance between the risk the organisation is prepared to take, and the costs to be incurred in targeted spending, to protect the organisation from cyber attack.
- Plan for resilience. As threats become more sophisticated, focus on resilience to attacks that get through, rather than preventing all cyber attacks.
- Be clear who is responsible for owning the risk, allowing for the dynamic and sometimes targeted nature of a cyber threat. Boards may consider giving one director specific responsibility for oversight of cyber risk.

"Tone from the top".

It is vitally important that the senior management team of any enterprise sets the right tone with regards to IT and Cloud risk management in it's messaging to the wider corporate population. This starts with a "risk appetite" that is communicated to people responsible for risk management. Senior management teams communicate the "tone from the top" on issues like cyber security through their messaging about appropriate behaviours and stressing the importance of training.

"Right to audit"/third party assessments.

The extended enterprise now encompasses all the organisations that either process data on behalf of the enterprise or outsourcers or consultants that have employees within the enterprise that have access to data and applications. It is vitally important that all aspects of the risk posed by these third parties are assessed by the extended enterprise and where required, a "right to audit" is exercised. This could take the form of asking a supplier to complete a questionnaire on issues like cyber security or data retention processes, or it could be a more intrusive on-site audit where representatives of the enterprise (including consultants) review the operations of a supplier against the agreed requirements. The choice here will often depend on the criticality to the business process and may even be a combination of questionnaire and on-site visit.

16. Institute of Chartered Secretaries and Administrators – Cyber Risk Guidance note June 2013

Legal responses and corporate policies

Service level agreements

Enterprises can use Service Level Agreements (SLA) to ensure that third party service providers meet all of their requirements when outsourcing to the cloud. The SLAs need to be robust, should not just be about service availability and should address other requirements such as but not limited to: compliance with Data Privacy or other data related legislation; detection and management of security events; end of life data destruction; and staff vetting.

Policies, processes and procedures

Most enterprises have policy documents that set out controls that manage various aspects of risk around IT and the Cloud. The quality and usefulness of these documents varies enormously. A good policy document will have been written by taking into account, the organisations risk appetite, the views of the target audience of stakeholders as well as taking input from industry good practice. It should be written in plain English and should be implementable. A good policy document will also generally require a sub-layer of process and procedure documents that set out exactly how a policy will be implemented. An effectively managed enterprise will regularly measure the implementation and use of policy, process and procedure documents to ensure their validity and usefulness.

Insurance

Cyber insurance is becoming a key response tool for managing risks in IT and the Cloud. The number of providers and types of insurance policy available in the market is increasing exponentially. As take up of these policies, and the volume of data on which underwriting decisions are made, increases the market is likely to become more competitive which should result in more attractive premium costs for the enterprise. Many enterprises are now buying cyber insurance that covers the costs of cleaning up after a cyber breach and some are also purchasing cover for loss of Intellectual Property or reputational damage. Some key issues with cyber insurance that should be considered are as follows:

- The most cost effect approach to buying cyber insurance is to undertake an effective risk management process that identifies risks that require cyber insurance and provide the underwriter with a quantifiable risk to minimise the cost of that insurance.
- In some countries (including the UK), it is illegal to buy insurance that covers the cost of regulatory fines; and
- Many cyber insurance policies will not cover the loss of data by third party suppliers.

Effective security management

Risk assessment

An effective estimation of IT and cloud security risk relies on an understanding of the impact, vulnerability and threat of different types of incidents and this needs three different types of knowledge and skills:

- An understanding of our organisation's strategy and business drivers;
- An understanding of the operational landscape – particularly with regard to technology; and
- An understanding of what is going on in the wider world of cyber space.

Risk assessment for IT and Cloud is a challenge because there are many types of cyber risk. Every enterprise will have a different risk profile as a result of the cyber threats that they face. The risks can be divided into five basic categories:

Censure and embarrassment, which is most relevant in highly visible industries such as retail, finance, media, or law impacts the company's brand through negative publicity in the media, and can have a significant impact on the bottom line of the enterprise. There will be direct costs and an indirect impact on brand and reputation that will typically be more significant but harder to quantify. For example, for the breaches of its PlayStation Network two years ago, Sony was fined £250,000 in the UK, but it has been estimated that the effect on its reputation was at least $1bn.

Client loss, where a company's brand is damaged, can affect revenue directly when customers choose to buy from competitors – churn in retail marketing speak. This effect is potentially even more significant for Business-to-Business organisations such as IT or professional services companies. If contracts or trust is broken by information being lost or stolen then there is likely to be a direct loss of revenue and often contractual penalties.

Direct fraud is mostly about losing money. Money is digital today and banks are fighting a continuous battle to keep their losses under control. Visa issued

a warning in January 2013 of a new wave of fraud based on targeted attacks. This affects any organisation that processes payments electronically. Fraud is also a problem for any organisation whose product can be taken in digital form – software, media and entertainment. 'Cybercriminals 'drained ATMs' in $45m world bank heist' BBC news 10 May 2013

Sabotage - generally, the two key targets of sabotage are online services and industrial systems. Many organisations have been hit by denial of service attacks on their websites including a sustained, sophisticated attack on US banks over first five months of 2013. This series of attacks appear to be political – but there have also been similar attacks for blackmail. The vulnerability of industrial control systems have yet to be exploited so heavily – except by the Stuxnet attack on Iran's nuclear programme. There is a potential future threat to key infrastructure – especially energy supplies but also manufacturing and transport. There are fewer organisations with a motivation for this kind of attack because it gets dangerously close to terrorism or even cyber warfare; however, there are a number of rogue states or terrorist organisations who may have the appetite and capability to launch a sabotage attack.

Cyber espionage is the silent copying of information for economic or political purposes. This is most relevant to industries with high R&D spend (such as high tech manufacturing, aerospace, software) but also: any enterprises competing for high value contracts (construction, mining), enterprises undertaking stock market reporting or enterprises undertaking M&A activity.

Threat intelligence

Risk assessment for an enterprise is more effective if the enterprise has good threat intelligence. This means having access to the types of threat faced by enterprises of similar size and scale, in similar market sectors, and enterprises operating in similar geographies. The extension of the enterprise means that senior management should also be cognisant of the threats faced by customers and suppliers. For critical business processes it is vital to have in place a robust risk based vendor assessment programme. In addition it is important for the enterprise to keep abreast of what is happening in cyberspace, the main threat actors and the techniques being employed in cyber attacks. A threat intelligence capability can be developed in house, though this is a luxury usually only open to the largest enterprises. Alternatively there are providers of general or tailored threat intelligence that can be engaged.

Data gathering for security event management

Enterprise security controls have in the past been developed on the basis of a "hard perimeter", a large wall in simplistic terms. This concept is now outdated as the boundaries of enterprises have extended beyond physical perimeters, are often opaque and cross international boundaries. It has therefore become paramount that the enterprise monitors its IT and Cloud estates for inappropriate or malicious activity. Being able to monitor the enterprise IT estate effectively means gathering significant quantities of log data from network devices and systems. Modern security monitoring solutions are increasingly becoming "Big Data" analytics engines capable of spotting anomalous activity in huge quantities of data.

Incident management

There is no such thing as perfect cyber security. An enterprise is very likely to experience a cyber attack at some point. However, like preparing the enterprise for a fire or a theft, it is the response when the attack occurs that will determine the impact on the enterprise. The early stages of an attack are often clouded by confusion as an incident progresses from suspicious activity to real impact. Initial breaches can be subtle and it can be difficult for IT staff to detect the significance of events or their potential consequences. By the time a response plan is formed, and senior decision makers are briefed, valuable hours or days may have been lost, increasing the impact. The key to security incident management is to develop a response plan which identifies key stakeholders and decision makers enabling a well coordinated swift response to an attack. Ensuring that there is a solid Business Continuity and Disaster Recovery plan in place which has been clearly communicated and is tested on a regular basis will minimize the impact of incidents. If the enterprise does not have the technical skills required, there are reputable organisations that can provide those services.

Summary

Information and communications technologies have brought significant benefits to enterprises and have been fundamental in enabling them to extend. Enterprises should continue to embrace the opportunities offered by mobility and cloud solutions to increase productivity and interactivity within the extended perimeter, but must be aware of the implications of their use. The new technologies have also changed the shape of the risk that the enterprise faces. The board of the extended enterprise must understand the size and shape of its own risk, must allocate responsibility for managing that risk and ensure the efficacy of that management, and should plan its response to the manifestation of a risk to ensure resilience.

Chapter 14: A practical approach to managing supply chain for the sector-level extended enterprise

Jake Storey, Roger Garrini, ManMohan S Sodhi

Summary

Our purpose is to provide a practical framework for Chief Risk Officers (CRO) of buyer and supplier companies, even competitors, in a particular industry that are part of the eco-system or the 'extended enterprise' at the level of the sector. These CROs would be able to collaborate with each other to minimise the impact of any supply-chain risk incident that could damage any subset or even all of the companies in the extended enterprise. Using the example of the aluminium smelting industry, we first describe what an 'extended enterprise' means in supply chain terms. Next we discuss how these companies in this extended enterprise can jointly share the risks they face that they could transmit to their customers. Finally, we describe what the individual players could do either to prevent risks from starting or respond to risk incidents they face to prevent transmitting them to their customers directly and to other companies indirectly in the extended enterprise.

Introduction

We seek to provide Chief Risk Officers (CRO) of companies a framework for managing supply chain risk that could become a 'systematic' or system-wide risk in their industry sector. Although companies are already using risk registers and different ways of assessing risk at the company level, our aim to focus on the inter-company dependence as regards managing supply-chain risk in the extended enterprise that could potentially include such entities as suppliers' suppliers, customers' customers and even competitors.

We propose that to understand and mitigate supply-chain risk at the extended enterprise level; risk managers should consider the following three steps:

- Identify the players in the extended enterprise,
- Identify and assess inter-company risks in the extended enterprise, and
- Mitigate the risks by preventing their origination or transmission.

It is clear that supply-chain risk is about the impact on a company from risk that can emanate from anywhere in that company's supply chain. However, the risk can come from sources from outside the company's supply chain but still within the same industry. For instance, with the Thai floods affecting Seagate, a hard disk supplier, chipmaker Intel's orders went down as computer manufacturers were disrupted on account of hard disk supply. Thus, although Intel is not a supplier to or a customer of Seagate directly, both are in the extended enterprise by virtue of their providing key components to computer manufacturers like Dell or HP.

The importance of collaboration

It is worth underscoring how risk has grown with changing buyer-supplier relationships. All organisations have suppliers in a complex interwoven web. Manufacturing, for instance, requires assembly and integration of sub-assemblies produced by a plethora of organisations. The subassemblies themselves are similarly composed of many parts and in turn these are supplied to the sub-assembly supplier. In very complex assemblies this often can go further and parts are supplied in many layers. Parts themselves are constructed from material and all rely on the provision of services and utilities to be able to deliver. This is true of hardware and software products and services. It is also true for financial services and the other professions, which rely on devolution of risk and on ICT supplier services.

These interacting buyers-and-suppliers are collectively known as the supply chain that, like any chain, is only as strong as the weakest link in it. A break in the flow of supplies in this chain could result in a company going out of business through no fault of its own.

Earlier, large companies tended to keep many suppliers

for each type of item purchased and were able to demand and expect to command their suppliers. Supplier failure would thus have limited failure. Successive newsworthy supply-chain failures have shown that damage need not always be contained – it can spread supply-chain-wide. This is because growing competition and investor pressure has resulted in fewer suppliers per purchased item, lesser inventory and tighter capacity. As such, the margins of failure are smaller than ever before and organisations can no longer depend on the survival of their suppliers to meet demands to deliver product. Indeed, large organisations can be put at risk by a component subsidiary fails to supplies parts to a supplier often several layers down the chain in a particular product.

Part of the reason for increased risk at different levels or tiers of supply is eroding margins and increased competition. Also, reliability of supply has forced many firms to consolidate their suppliers and develop closer relations. Freedom of choice balanced against the cost of having to choose efficiency suggested that fewer suppliers meant less procurement staff, smaller numbers of accounts, less data, and less supervision, which meant lower overheads for the purchasers.

Also, as large companies faced stiffer competition globally, their purchasers squeezed suppliers harder on price, expecting more for less. Eventually suppliers, who had tailored their business to meet the bespoke requirements of the large purchaser, failed. From the large purchasers' viewpoint, lower prices were possible only with economies of scale so lower prices meant fewer suppliers anyway so supplier failures were inevitable. However, another possible outcome is that some other group acquires the supplier, which now becomes more assertive and requires increased prices or simply refuses to supply at inappropriate prices. Similarly, if a supplier realises that it is in a catastrophic position with a contract and decides to default and return all revocable funding. The purchaser thus acquires risk from its own aggression.

The aim of this chapter is to present how to make collaboration possible for managing supply chain risk for the 'extended enterprise' as a whole. We use the example of the aluminium industry in Europe for illustration as how such a collaborative effort could be made to work in practical terms.

Using industry associations for mitigating supply chain risk

The 'extended enterprise' is a nebulous notion. Indeed, depending on the context, any company belongs to a different extended enterprise. For supply chain risk, we naturally consider supply chains as being part of the extended enterprise for mitigating the risk.

How could a company bring together its extended enterprise together for this purpose? To make this tangible, consider the International Aluminium Institute and its committees such as the Bauxite and Alumina Committee. Such an industry group has the benefit of having already evolved to get past anti-trust issues and also of having companies in the extended enterprise already as members. In this report, we envisage the idea of extended enterprises based on supply chains working together to mitigate supply chain risks that affect them jointly – hence the need for collaboration as discussed in the previous section.

One practical idea for managing systemic supply-chain risk can dovetail into what such industry associations already do: carrying out a survey of members using questionnaires, such as the one for collaborative and competitive efforts on the technology front by the International Aluminium Institute (2010). Mitigation of supply chain risk can be understood as competitive as well as collaborative efforts to motivate joint efforts where necessary.

Below, we first provide a background of aluminium production and then describe three steps that an extended enterprise of a group of interested companies could carry out to make their risks visible to their respective customers and what steps they would undertake to protect the customer.

Background: aluminium production

Consider the aluminium production extended enterprise starting from mining bauxite (a mineral rich in aluminium oxide) to delivering 'billets' for further processing. In 2005, the People's Republic of China was the top producer of aluminium with almost a fifth of the world's production, followed by Russia, Canada, and the USA, reports the British Geological Survey. Our focus in this article is on production in Europe.

To enable further discussion, we describe some terms below:

Liquid pitch - This is made from refining coal tar, which is a by-product derived from coal carbonisation when

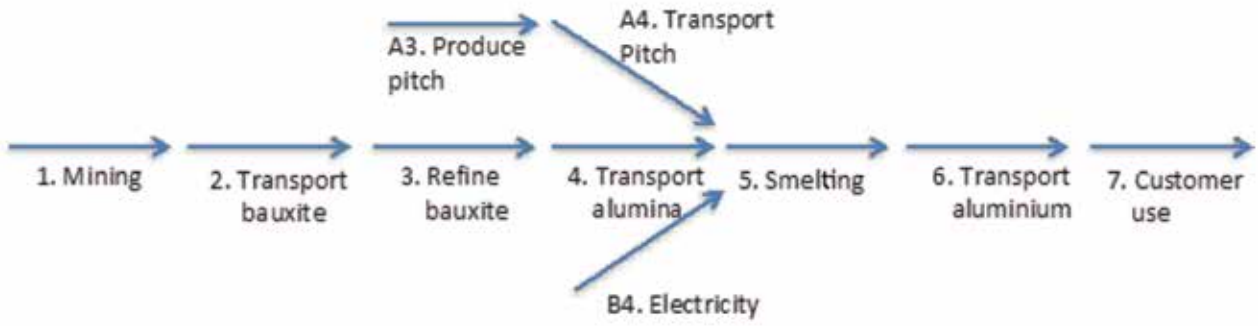


Figure 14.1: Extended enterprise for aluminium with different parts of the value chain

making coke. The pitch is transported in high heat form as it is carcinogenic in solid / powered form. The pitch is used to make the anodes used in the smelting of Alumina. There are coke plants around the world – including China, Australia, UK, USA Southern Africa, Denmark and the Netherlands – that supply pitch.

Bauxite - This is the 'ore' for aluminium mined from the ground. It is further refined into alumina using the Bayer process / pressure and filtering.

Alumina – Obtained from bauxite, this is the main input for the creation of Aluminium, which is created through electrolysis / chemical process (cheap and ready supply of energy is the key component) called the Hall-Héroult process.

Processing - The Hall-Héroult process is the major industrial process for aluminium extraction. In the Hall-Héroult process, alumina is first dissolved into molten cryolite, a chemical compound of aluminium and sodium fluorides, with calcium fluoride and then electrolytically reduced to aluminium at a temperature between 950 and 980 °C (1,740 to 1,800 °F). Aluminium electrolysis with the Hall-Héroult process consumes a lot of energy, but alternative processes have thus far been found to be less viable economically and/or ecologically. The Hall-Heroult process produces aluminium with a purity of above 99%.

Both of the electrodes used in the electrolysis of aluminium oxide are carbon (hence pitch made from coal tar). Once the refined alumina is dissolved in the electrolyte, it disassociates and its ions are free to move around. The aluminium metal then sinks to the bottom and is tapped off, usually cast into large blocks called aluminium billets for further processing. The carbon anode is consumed by subsequent reaction with oxygen so the pitch has to be replaced. The anodes in a reduction cell must therefore be replaced regularly, since they are consumed in the process. The cathodes do erode, mainly due to electrochemical processes and metal movement. After five to ten years, depending on the current used in the electrolysis, a cell has to be rebuilt because of cathode wear.

Energy - Electric power represents about 20% to 40% of the cost of producing aluminium, depending on the location of the smelter. Aluminium production consumes roughly 5% of electricity generated in the U.S. Smelters tend to be situated where electric power is both plentiful and inexpensive, such as the United Arab Emirates with excess natural gas supplies and Iceland and Norway with energy generated from renewable sources. The world's largest smelters of alumina are People's Republic of China, Russia, and Quebec and British Columbia in Canada.

We now describe the three steps companies in the same sector or rather the same 'extended enterprise' can take:

Step 1: Identify the extended enterprise

Consider the following extended enterprise with most of the players within the European Union (EU). In our case, the extended enterprise comprises the players in the supply chain at different stages of production (Figure 14.1).

The various players are listed in Table 14.1. Note that the 'extended enterprise' can be bigger or smaller depending on the CROs who wish to discuss their supply chain risks and coordinate their actions on this front with a view to minimise harm to the extended enterprise rather than maximize their own company's profit or their total profits across all the companies in the extended enterprise as defined.

These companies face risks that can have effect not only on them but also on the other companies in this

Table 14.1 A (partial) list of players in different parts of the extended enterprise, in the order of the different steps in the value chain

COUNTRIES WITH MINING OPERATIONS	MINING COMPANIES	SMELTERS IN AND OUTSIDE EUROPE	PITCH TRANSPORTERS
Jamaica Brazil Guinea India China Australia	BHP Alcoa Rio Tinto Norsk Hydro Chinalco	**With European operations:** Rusal Alcoa Rio Tinto/Alcan Aluar **With global operations:** Alcoa Alba Rio Tinto Alcan Albras Hydro Emal Dubai	Gearbulk Stolt COSCO Vroon TSA Sargeant Marine Wisby

extended enterprise. If the CROs of these companies were to meet to discuss the long-term health of the extended enterprise by way of minimizing impact of the extended enterprise as a whole of any risk incidents, they would need to specifically discuss the type of disruptions and where they originate as regards the extended enterprise. They not need to discuss risks that affect only their own companies (as per their risk registers) but not others.

Step 2: Identify and assess inter-company risks in the extended enterprise

For the aluminium production extended enterprise (Figure 30), the risks originating at or transmitted by the individual players (or more generally as representing their category as miner, producer, transporter or customer). Table 14.2 lists the risks originating with the transporters and impacting their immediate downstream partners; Table 14.3 does the same for smelters; Table 14.4 for mining and refining; and finally, Table 14.5 for the producers of pitch.

The manufacturer-customer can also cause risks to the upstream suppliers by lowering demand and by distorting the expectation of future demand (bullwhip effect).

Step 3: Mitigate the risks by preventing origination or transmission

In the network of companies in the extended enterprise, risks can only be mitigated by preventing starting them and by preventing from being transmitted to other companies. That way disruptive shocks will either not happen in the first place, but if they do, they would not be transmitted on to other players. This combination will minimise the impact on the extended enterprise and ensure the long-term health of all the companies in the extended enterprise.

With the risks already identified (Tables 14.2-5), we can start with each company showing what it has done or is doing to prevent a risk incident from originating on any of its locations as well as what it is doing to prevent transmission. Tables 14. 6-9 can be used as a starting point for collaboration among the different supply-chain players, with each party explaining to its immediate customers what it is doing to keep them from harm. In turn, they can see what their suppliers are doing to protect them from risks originating at these suppliers.

In addition, it is incumbent on the end-customers to keep the upstream supply chain partners informed about its own status and any risk incidents.

Table 14.2: List of risks originating with transporters and the impact on immediate downstream partners

LINK	ACTIVITIES	RISK(S)	CAUSES	IMPACT
2	Transportation of	Piracy	Sailing through the Gulf of Aden. Poor security measures	Delay of shipment of bauxite
4	Transportation of alumina			Delay of shipment of alumina
6	Transportation of aluminium			Delay of shipment of aluminium
A4	Transportation of Pitch			Delay of shipment of Pitch
A4	Transportation of Pitch	Political	Sailing in the Middle East / Act of War	Delay of shipment of pitch could close the Aluminium smelter
2,4,6, A4	All of above	Port Congestion	Weather, size of port, strikes (bank holidays) and number of vessels calling at the port	Delay of shipment

Table 14.3: List of risks originating with smelters and the impact on immediate downstream partners

LINK	ACTIVITIES	RISK(S)	CAUSES	IMPACT
5	Smelting	Disruption of Power Supply / Unable to smelt the Alumina	Energy supply is disrupted (fuel supply gas, coal, hydro or thermal). Could be for a variety of reasons such as environmental (earthquake)	Not able to produce Aluminium
5	Smelting	Labour	Poor labour relations	
5	Smelting	Unable to obtain raw materials	Lack of resilience in supply chain	

Table 14.8: List of risk-mitigation steps originating with bauxite mining and refining to protect downstream partner

LINK	ACTIVITIES	MITIGATION STEPS	LINKAGES - SUPPLY CHAIN	LINKAGES - EXTENDED ENTERPRISE
1	Mining	CSR / HSE and legal compliance procedures	Co-ordination with mines, smelter and shipping company / stockpiles	Alternative supply of bauxite that is not encountering this problem
1		Employee surveys, bench marking T&Cs, good T&Cs, and good union relationships		
1		Lobbying, and strong legal compliance procedures		
1	Transportation	Alternative load / discharge ports. Appropriate stock carrying levels		
3	Smelting	BCM plans, alternative power supply/ (back up generators, alternative smelters	Co-ordination with mines, smelter and shipping company	Supply / demand - market priced considerations (i.e. buy and cover from the market)
4	Transportation	Alternative load / discharge ports. Appropriate stock carrying levels		

Table 14.9: List of risk-mitigation steps originating with pitch producers to protect downstream partner

LINK	ACTIVITIES	MITIGATION STEPS	LINKAGES - SUPPLY CHAIN	LINKAGES - EXTENDED ENTERPRISE
A3	Producing Pitch	Good environmental safety procedures	Co-ordination with mines, smelter and shipping company	Alternative sources of pitch supply / reserve capacity
A3	Producing Pitch	Lobbying and good compliance procedures		
A3	Producing Pitch	Good HSE procedures and (safety) culture		
A3	Producing Pitch	Employee surveys, bench marking T&Cs, good T&Cs, and good union relationships		

Conclusions: Implications for risk practitioners

Using the example of an extended enterprise by way of aluminium billet customers in the EU, we have showed how companies should behave in this 'ecosystem' – howsoever scoped by geography or by association – by focusing on risks that are strictly at the inter-company level. These are risks originating at one company or being transmitted by that company to other companies that are 'in scope' of the chosen extended enterprise.

In order to be able to effectively collaborate within the extended enterprise to mitigate supply-chain risk, it is important that companies understand their universe from a supply-chain perspective. This is possible only if all parties seek to know and understand risks and risk management efforts of their major suppliers (one tier below) in the supply chain – if all parties do this jointly, the entire extended enterprise becomes more robust as result. Such alignment between buyers and suppliers must eventually be based on shared values and ethics, incentives, as well as the sharing of information, risks and the mitigations in place. Thus the key to mitigating risk is collaboration and we have provided a practical way to make this possible.

Chapter 15: Relationship risk management: perception or pragmatism

David E Hawkins, Institute for Collaborative Working

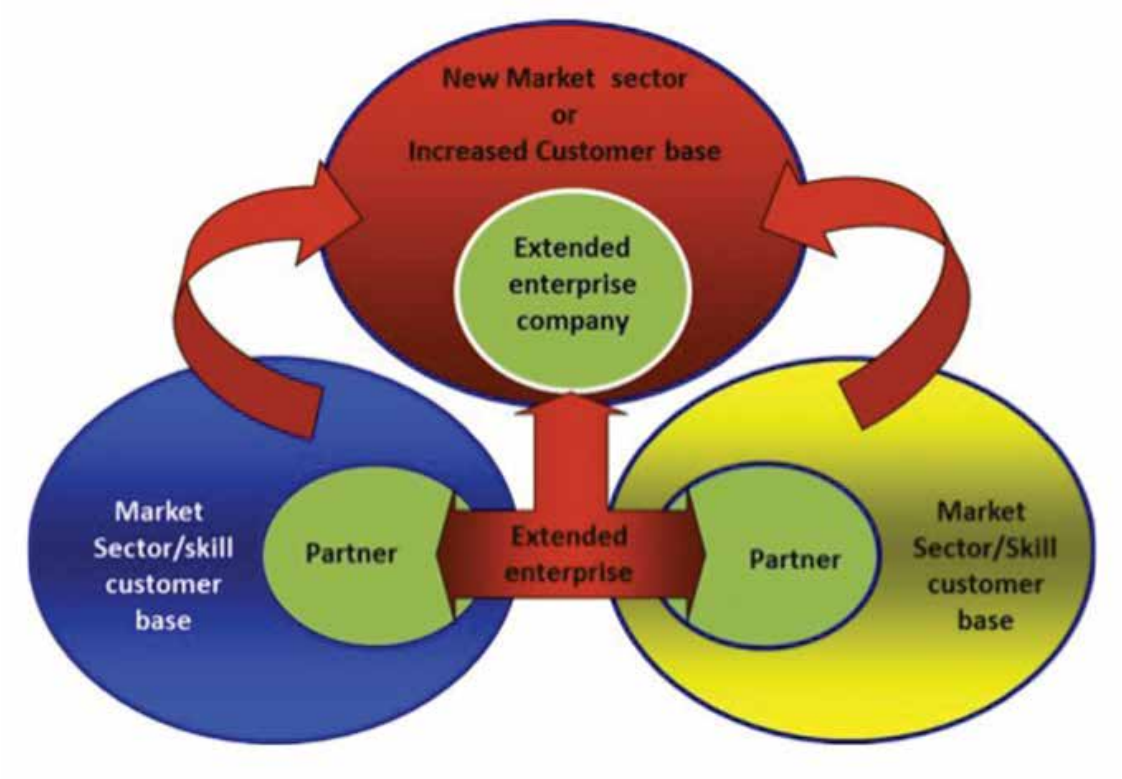


Figure 15.1: Complex delivery models

In the past three decades we have seen a significant transformation of the business world, with the growth in mergers & acquisitions, global sourcing, outsourcing, consortiums, alliances, partnerships, public private partnerships, collaborative networks and the emergence of what today is often referred to as the extended enterprise.

These complex delivery models are being driven by both the quest for more competitive performance and the pressure to create more expansive business propositions. Simultaneously the explosion in technology has both closed the communications gap between organisations whilst at the same time delivering greater transparency in terms of social media and corporate reputations. The interdependence of organisations is perhaps more prevalent than ever before as too is their vulnerability through these alternative business models.

The lack of focus on relationships may in part be a reflection that traditional business models where based largely on internal capabilities but as the outside in theory suggests (see Figure 15.2) these have given way to extended interfaces but have still mainly relied on contractual safe guards.

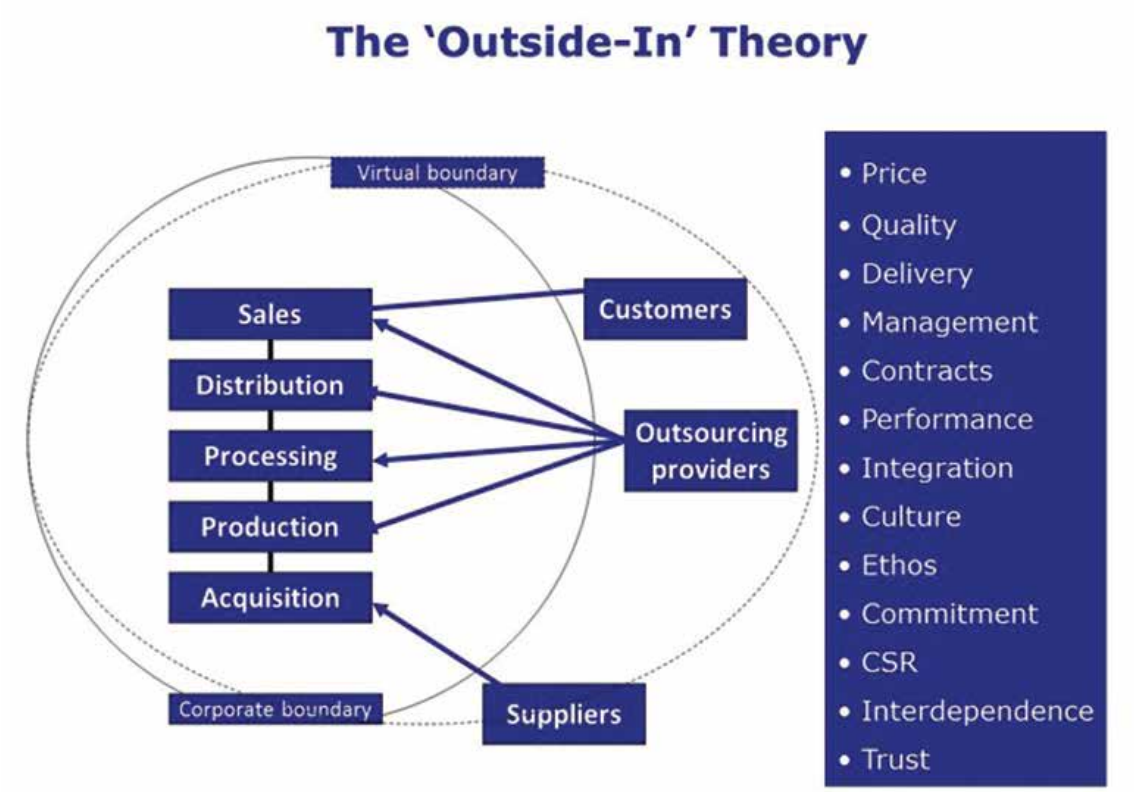


Figure 15.2: The ICW 'Outside in' theory

It is now generally accepted that 60%-80% of operating costs for the majority of company sits outside their own organisation. At the same time the evidence from a wide variety of surveys and reports suggest that as many as 80% of mergers and partnerships are deemed to be failures or at least fail to deliver their full potential. Against this background we have also witnessed the emergence of what one might call ***'perception based economics'*** where the value of a company is based less on its assets and more on speculative assumptions. There has always been recognition that Good Will represented the intangible reputational value between tangible assets and market value. Yet today based on even a conservative perspective of these extended operating models the intangible far outweighs hard assets and the performance of these extended networks is a key factor in delivering outcomes.

Today the buzz word is *'collaboration'* whether from Government, public sector or industry Collaboration is the answer but what the question. What is obvious it that as we have embraced technology the real asset perhaps more than for business remains sustainable relationships. The implications of relationships in business and the spectrum of inherent risk that a failure to manage relationships effectively can have on organisations the overall risk profile and whilst relationships are a fundament aspect of all business activities and yet they seldom gain recognition when considering risk assessment and/or management.

Risk pervades every aspect of business whether investment, product development, operational performance, reputation or supply chain. The one exception perhaps in many organisations is the customer relationships where the focus is on retention. In business it is generally accepted that the more risk which can effectively be managed the greater the competitive advantage. On the other hand by simply seeking to transfer risk there is frequently the potential to increase risk when the issues are outside the capability or influence of those given the risk. Risk in this context can be generically categorised by financial, performance, safety and external events whether natural or social/political (see Table 15.1 below).

The one aspect that is seldom mentioned in any risk brief is those associated with relationships. This should raise concern to business leaders since the most likely failure of any business activity is likely to emanate from the breakdown of relationships such as between customer, partners or suppliers. The frequent assumption is that by focusing on contractual conditions and liabilities places this risk in a manageable position

but perhaps ignores the reality that once the contract is invoked failure is largely assured. Even in the most integrated of business activities where risk is openly and jointly managed the aspect of relationship risk is seldom identified as a key consideration and left to perception.

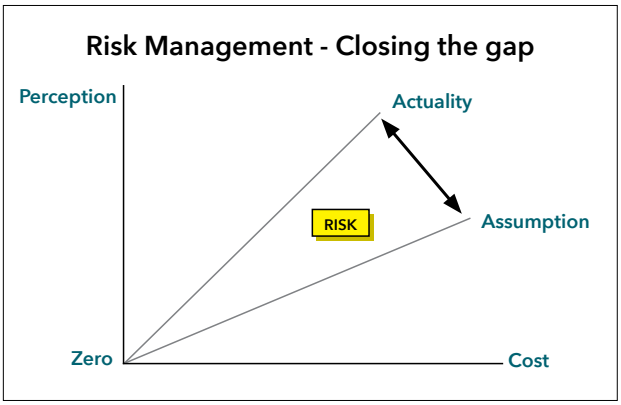


Figure 15.3: Risk management - closing the gap

As the business landscape becomes more complex and challenging, the relationships between organisations also takes on new and varied configurations. It has generally been accepted that for most organisations they are both customer and supplier in relation to different aspects of the value chain. The growing trends in globalisation and convergence in many industrial sectors has introduced the vista of trading relationships both vertically and horizontally within the value creation process. It is becoming more frequent to see competitors working closely together in specific ventures, as well as the complexities of mergers bringing together previous competitors into a single organisation.

The publication of BS 11000, the world's first Collaborative business relationship management

Figure 15.4: BS11000

standard, created a framework which can be deployed in any context where relationships are recognised to be a significant factor. Developed through pan-industry consultation it provides a structured approach to building more sustainable relationships throughout the value chain to ensure relationships are effective and sustainable by establishing organisational engagement rather than dependence solely on potentially transient personal interfaces. To consider the application of the framework in the context of risk the following highlights some risk aspects that flow thought the standard.

Awareness: For relationships within any business to succeed and have traction they need executive sponsorship and policy to give direction, support and defused internal frictions when considering external engagement, which can often be a cause for major performance risk. Organisations need to focus their efforts towards those key relationships to avoid dilution of resources. The backbone of the framework

Table 15.1: Relationship risk considerations

Operational	**Performance**	**Technology/IPR**	**Stakeholders**
Reputational	**People movement**	**Process conflicts**	**Knowledge fusion**
Behaviours	**Culture**	**Disputes**	**Change**
Business continuity	**Environmental**	**Transition**	**Future proofing**

is a relationship management plan which articulates the corporate requirements when collaborative approaches are being considered.

Knowledge: The failure of many so called partnerships can emanate from poor development of a sound business case which underpins the rationale for integration and the ability to measure success. At the same time the greater the integration the more focus should be placed on exit strategies to address business continuity risks and understanding the potential risks of knowledge creep or loss of skills.

Internal assessment: As outlined above in the outside in theory whilst organisations may recognise the value of relationships their operating models are fundamentally based on traditional command and control. Where performance is reliant of external resources these models are inherently risky. To manage the risk in these alternative business models there is a need to ensure the policies, processes and skills are in place to exploit joint capabilities.

Partner selection: The choice of partner is crucial since by association both performance and reputation are inextricably linked. Yet as already mentioned the failure to consider cultures, behaviours and values of partners has likely been the cause of many failures and thus increased risk, as is the failure to recognise and align the individual objectives of the parties.

Working together; Organisations can today communicate, interact and exchange data via technology but the governance of these integrated relationships is frequently less well managed. Internal and external tensions may be continuously pulling in different directions risking operational weaknesses together with process conflicts impacting outputs. Operational management structures need to be fully assessed and adequate focus placed on embedding the right behaviours to target joint performance.

Value creation: Perhaps the biggest risk with these alternative models is complacency which combined with any churn of people tends to plateau or degrade. Thus it is crucial to maintain a drive to build the relationship around continual improvement and add value over time.

Staying together; the day to day management and monitoring of the relationship is critical if the risks of failure are to be avoided. Performance measurement is normal practice but measuring relationships and building trust is a key along with effective management of disputes which will inevitably arise at some point. Risk in itself is a critical influence on behaviours and joint risk management including relationship issues is essential.

Exit strategy: Markets change as do economic and political influences leading to re-focusing of the relationship at some point. With this in mind any collaborative relationship needs to be aware of the implications and risks associated with disengagement.

Conclusion

If we are to exploit the potential of the extended enterprise we cannot ignore the potential impacts on risk management. More importantly in the broader sense of managing business risk the implications of relationships are not something that can be left to chance. Relationships link every aspect of business and yet for many they have a limited focus for those that are charged to manage risk and deliver performance. If we do not recognise the implications of relationships then much of what is put in place to drive business outcomes and create more effective opportunities for stakeholders is inherently flawed.

Since the earliest of times business has been fundamentally balanced on the ability of traders to build relationships on which they can rely. As we have built more sophisticated business models we have progressively placed our trust in legal contracts, which remain an integral aspect of business today but they will seldom on their own deliver success. Relationships are an integral part of business which in turn should make them a key aspect of risk management to drive a cohesive approach that will underpin the desired objectives and outcomes.

Key questions

- How critical are relationships to your business?
- Is there a senior executive responsible for relationship management?
- Do your risk management processes include those risk associated with relationships?

Additional reading

BS 11000-1_2010 collaborative business relationships- Part 1: A framework specification

BS 11000-2_2011 collaborative Business relationships- Part 2: Guide to implementing BS 11000-pt1

'Raising the standard for collaboration' published by BSI 2013

Case study 1:
Joint risk management for mutual benefit

Roger Garrini

The vulnerability of major manufacturers to supply chain failures grows. In complex developments it is not enough to simply place the order and wait. In former times with sufficient financial slack and cost plus contracts, it was easy to place, and hide behind, a fixed price contract for a development item and rely on the price and profit incentives to manage the contract. This worked when the supplier was big enough and had sufficient funds and the waiting time was absorbed in contracts by accepting delay. This is no longer true.

The move to single sources as a way to cut down the number of suppliers and improve supplies was fine too, in principle. Financially it looks sound and it is based on good relations between the partners. But that protection breaks down when the major project depends on the (usually small and specialist) supplier and, despite the watertight fixed price contract, the supplier cannot, for whatever reason, supply.

In this example from the aerospace industry, a carefully worded fixed price contract for a laser had been placed by a large purchaser exclusively with a small specialist supplier, who was working with state of the art of laser design. The laser was required as part of a technology demonstrator of an airborne system, itself contracted at a fixed price.

The relationship between supplier and purchaser was sound and friendly but it became increasingly obvious that the supplier was in financial difficulty due to other contracts outside the project. Further, they were also in technical difficulty as the supplied lasers continually failed at the integration stage when run for more than a few minutes. The integration stage consisted of a complex three week alignment and adjustment phase under laboratory conditions with a team of three working full time. It seemed that just as the alignment produced some useful performance the laser would fail again.

Every time this happened there was a four week delay while a transistor was replaced and the laser re-tested for release again for the integration trial. Several iterations of failure and months of delay had been incurred when the combined design teams finally diagnosed that the problem was a heat build-up somewhere in the laser. The cost of the delay to the purchaser ran into thousands of pounds every week due to the delay and re-work as well as maintaining their project team.

The specialist supplier asked for help. It would have been easy for the purchaser just to use the contract and insist that the supplier fixed the problem but it was realised that this would have broken the supplier to no purpose.

It was decided that the purchaser and supplier would work together to find a solution. Elsewhere in their business, the purchaser had infrared cameras and these were brought in for a bespoke set up to run the laser and look for the heat source. After an hour or two it became clear which transistor was causing the problem and investigation and support from the purchaser's mechanical team showed that a simple heat sink would resolve the issue. The laser became reliable and the project began to move forward again. The heat sink cost just a few pounds! The extra effort was a few hours of work using facilities which existed in the purchaser's factory. Further delay would have cost thousands of pounds more if the purchaser had stuck to the letter of the contract.

Suppliers, once chosen, are part of the family for the project and should be nurtured. If risks are visible and information shared, joint solutions can be found. This case shows us that managing risk in an extended enterprise requires a flexible approach, attention to relationships and an understanding of the motivations and interests of the different parties involved.

Case study 2:

Heathrow Terminal 5 - a new paradigm for major programme risk management

Jeremy Harrison, Mike Bartlett

Through the 1990's the general sentiment in the construction industry was that major complex projects overran schedules and exceeded budgets. Reports such as Latham (*"Constructing the Team"*[17]) and Egan (*"Rethinking Construction"*[18]) endeavoured to promote a new approach to engaging with the supply chain and managing risk.

With this as a background to the imminent construction of its massive Terminal 5 Project, BAA developed an innovative delivery model. It created a unique contract between itself as client and its delivery partners (*The T5 Agreement*) which articulated a different approach to transparency and collaboration in managing risk and underpinned this with an alternative, holistic "all parties" approach to project insurance. Books have been written lauding the delivery methodology and even now, 6 years after completion, people who worked on the project at all levels talk proudly of their experiences and it is used as a case study in academic and professional circles.

Since completion of T5 in Spring 2008, on time and within its budget, no other project has utilised the T5 delivery model. Perhaps its construction success and hence a desire to emulate its approach has been overshadowed by the operational difficulties at opening that grabbed the headlines. Industry opinion is certainly divided as to whether the project is a success or a failure[19]

Many client organisations are implementing or at least testing a "partnership" approach between client and delivery partner(s) but by bolting this on to standard contracts and insurance strategies. The Olympics in 2012, the UK's most prestigious major construction programme in recent years, was an outstanding success using a partnership model for construction delivery but relatively standard contract forms and insurances.

Perhaps the financial crisis, which started in Autumn 2008, soon after T5's completion, changed the construction environment to obviate the need for radical delivery models. It would certainly appear that the need to acquire turnover in the construction industry since 2008 has created a much more benign commercial environment. Actual construction costs have proved year on year to be lower than inflationary predictions and there have been few headline grabbing overspends and delays as witnessed in the 1990s.

Are we being complacent? Is the corporate commercial experience – if influenced only by the last 6 years of construction performance – blinkered? Is the desire for construction turnover and low inflationary pressure creating a bubble that could burst at any time?

Perhaps clients with major long term programmes should be contemplating the scenario of a significant construction climate change and develop a strategy to pre-empt and provide a basis for mitigating any reversion to the destructive contractual environment of the 1990s.

This report explores the T5 approach to Risk Management – both the direct physical actions undertaken and the psychological implications – and suggests what aspects could be refreshed to incorporate more recent thinking and adopted to deliver a next generation paradigm in major Programme Risk Management.

Heathrow Terminal 5: background[2021]

The 5th Terminal for Heathrow Airport was first proposed in a White Paper in 1985 in order to provide much needed additional capacity for the UK's only hub

17. Constructing the Team, Latham M, HMSO, 1994
18. Re-thinking Construction: Report of the Construction Task Force, Egan J, HMSO, 1998
19. Terminal 5: Success or Failure, University of Brighton, 2012
20. Heathrow's T5: History in the Making, Doherty S, Wiley, 2008
21. Heathrow Airport Terminal 5, ICE Proceedings Vol 1, May 2008

airport, to relocate British Airways to one terminal from its split T1/T4 operation and to enable the whole scale reconfiguration of Heathrow from its original inefficient 'Star of David' layout to a modern multi-functional 'toast-rack' layout.

The complexities and interfaces for such a major scheme, with necessity for a new M25 interchange and relocation of a major water treatment works meant that planning permission was only granted in 2001 after the longest Planning Inquiry in UK history.

Advantage was taken of the protracted authorisation process to develop the methodologies (procurement and logistics) for completing the project in the most efficient duration – once Planning was granted – and a budget which would be truly representative of a final cost.

The construction environment throughout the 1990's was filled with perceived failures such as Scottish Parliament, Jubilee Line Extension and The British Library and BAA considered how this environment could affect T5: "*If things go as they normally do on major UK construction projects, the statistics say that T5 could be 3 years late, 80% over Budget and 6 people killed*"[22]. BAA elected to develop a new approach to managing the risk.

The opening date of 30th March 2008 was set in 2001 and a budget of £4.3Bn agreed in 2003. As a private sector client this investment constituted two thirds of BAA's capital value. If the budget was wrong the very viability of the company could have been jeopardised.

The construction site, the largest in Europe at the time, covered 260 hectares, the size of Hyde Park. 8000 people were employed on site at its peak across 18 projects by 80 first tier suppliers.

The extended enterprise of the T5 Project is reflected by 20,000 lower tier suppliers involved in the project's success, 30 airlines affected either directly or indirectly by the project's impact on operations and the innumerable stakeholders who submitted or desired production of the 5900 public inquiry documents.

The project opened in 27th March 2008 3 days ahead of the 2001 schedule and was within the £4.3Bn budget set in 2003.

T5's approach to risk management

The two pivotal components of the T5 delivery strategy to manage risk innovatively were the T5 Agreement and the T5 insurance strategy. Together these promoted the philosophies of:

- All risk on client: BAA held all the risk all of the time but with clarity about liability for cost impact separated from who is harmed by the risk
- Shared liabilities: all parties to the agreement share in the cost impact of risk on a strict no-fault basis with caps for the ability for any party to bear the cost impact and supported by commensurate insurances
- Cultural Commitment: the unusual nature of the agreement with explicit requirements on individuals and companies to be aware of and support each other through both formal partnerships and supportive behaviours of trust and cooperation created a strong psychological contract.

T5 Agreement

"The T5 Agreement: a totally new form of contract agreement… BAA carries all the risk and is insured for all that risk. If any problems arise the answer is not to find someone to carry the can but to work together to find a solution.

"It's the most important enabling strategy we have… it is far more than a common contract. It gets you over a number of emotional hurdles at higher levels."[23]

The Agreement was 260 pages long which is comparable, if not less than, industry standard contracts on other major programmes once corporate and project specific amendments are incorporated. For example, the contract for Network Rail's Thameslink Programme constitutes 319 pages. The T5 Agreement also had the advantage of being a stand alone document as opposed to most 'standard' contracts, which for copyright and/or contractual precedence reasons tend to be split into at least 3 volumes (e.g. standard contract, corporate/ project amendments and preliminaries), making them very complex to follow.

One of the most fundamental differences between the T5 Agreement and a standard contract is that multiple parties (namely the key delivery organisations) to the Programme were signatures to it. It is also

22. Heathrow's T5: History in the Making, Doherty S, Wiley, 2008
23. Heathrow Airport Terminal 5, ICE Proceedings Vol 1, May 2008

significant that the Agreement was signed by the Companies' Managing Directors rather than their legal representatives.

Although BAA were still clearly the client, the multi-party contract emulates partnering concepts by replacing a traditional client/ contractor hierarchy with an all-equal team which creates a psychological effect to promote risk sharing amongst the parties. Having the operational directors sign the Agreement perhaps created a much stronger moral commitment to driving success as opposed to a separation between the execution of physical works and an obscure contract perceived to be protecting the party's liabilities. It was certainly evident that company executives felt the obligation to resolve any issues arising personally.

The Agreement has all the requirements of a Contract: what is required from each party by when; how costs will be reimbursed; each party's rights in the event of a dispute and how such disputes would be resolved. There is no underlying contract form though the drafting is similar in many respects to the (then current) NEC Contract and this would probably have been used should any dispute have escalated to require external judgement. In the event this is a moot point as no disputes escalated to this level – an accolade for a programme of this magnitude.

The Agreement continually reiterates the importance of:

- Interdependent parties collaborating to deliver the project and to manage risk for the common good of the project;
- Sharing the risk of failure
- Shared decision making particularly in relation to costs, responsibilities for implementation, payment,
- Parties being transparent and particularly regarding risks they may be aware of;
- Parties being non-adversarial
- Integration and overlap of design and construction

A cost reimbursement model was incorporated so that only actually incurred costs were paid for (with a fixed overhead and profit margin). To validate costs BAA found it necessary to introduce a cost verification system administered by a 3rd party.

Contingencies for risk impact were established (related to perceived exposures) and allocated to each Project Team and this was drawn down by the collective team in accordance with the actual evidenced impact. If the cumulative risk impact was ultimately lower than initially envisaged, the parties to that area of the programme collectively shared in the saving.

In addition there was an incentive scheme based on achieving progressive schedule milestones, funded from a contingency commensurate with the cost impact of delay risk.

In the event of cost excesses greater than budget plus contingency, BAA would reimburse but the ability for any company to earn profit on the excesses was constrained.

Insurance strategy[24] [25]

The philosophy for insuring the project was to cover all primary parties to the Project on a joint basis with no necessity to determine a single point of blame (i.e. "no fault" basis).

This covered Construction "All Risks", 3rd Party Liability and, in a first for the construction industry, all Parties' Project Professional Indemnity.

Excesses on each policy in the event of an insured incident were attributable to a Project Team rather than an individual party thus reducing the potential to try and transfer liability to another party within the team.

The advantages of a project-wide owner controlled insurance for "Construction All Risks" such as to assure adequate coverage across all the supply chain and interfaces, provide an economy of scale and simplify claims management are well recognised and this approach continues to be used by many construction client organisations.

Likewise an owner controlled policy for 3rd Party Liability is commonly used by clients to assure adequate coverage for 3rd Party risks and was particularly important for BAA's construction teams as they worked in close proximity to expensive aircraft and sensitive airport operational systems.

The all Parties' Professional Indemnity cover for redesign and/or reconstruction arising out of any defect in design remains unusual in construction, though policies are still available[26]. The advantages are the same as those for the other covers; e.g., economy of scale, adequate

24. T5 Risk Management Summary, Bartlett M. BAA 2006
25. Heathrow's T5: History in the Making, Doherty S, Wiley, 2008
26. Willis, Owners' Protective Professional Indemnity (OPPI)

coverage across all suppliers and simplified claims' management. However there are two particular aspects of the PI coverage to note:

- Designers appeared to be much more open to collaborate with contractors and solve issues rather than be protective over corporate liability[27];
- Resolution of design issues was much faster than can typically occur if a project has to stop and wait for separate insurers to resolve who is liable (in practice it is probably rare for a single party to be wholly liable and clients will have to cover some of the costs)[28];

One downside identified on T5 was that the cost savings from the owner controlled policy (i.e. that suppliers would reduce their costs on the basis that they did not have to provide the insurance cover) were difficult to extract from 'global' policies or general overheads.

Construction industry: what is the current prevailing environment and what is the status of risk management?

Economic conditions 2008 to date

In the first half of 2008 construction costs were continuing their pattern of several years and rising month on month with forecasts projecting this to continue for the foreseeable future[29]. However, in late Summer 2008, it became apparent that the growing global financial crisis would indeed affect UK construction. By November, 2008 there was an almost complete halt in house building in the UK and construction contractors began to worry about maintaining turnover volumes and profit expectations.

BAA's response to this paradigm shift was particularly interesting. The company reconsidered what actual inflation might impact construction forecasts by developing a bespoke inflation index for Heathrow construction activity and removed uncommitted general inflation provisions across its projects[30]. This action ring-fenced approximately 10% of 'costs to go'.

Since 2008, tender prices have stayed very competitive and whilst forecasts have suggested that inflationary uplifts are required, in practice, actual costs have continued to be lower than these expectations[31].

There is a danger that this inflationary windfall has masked degradation or at least a failure to improve general management of risk. From a budget of £9.3Bn set in 2007 prior to the economic crash[32], the Olympics returned £528m[33] which at just over 5% is approximately half what BAA achieved.

Now we are in 2014, there are a number of indicators to suggest the construction economy is turning again. There is a growing body of evidence that the general UK economy is improving. House prices have been rising for several months. The likelihood of an interest rate in the next 12 months is growing. Unemployment is dropping and the general mood in the UK and Europe is more optimistic than has been seen for several years.

Perhaps we are on the cusp of a boom period for construction – major public spend on infrastructure projects is seen by the current UK Government as a key component to support economic recovery. If the supply chain has been operating in a repressed state with years of underinvestment, the limited remaining capacity may now be able to charge a premium for its services.

Wage agreements for many of the major construction trades have been below inflation for several years, reflecting the restricted availability of work. If the market has indeed turned, it is likely that individuals will believe rate increases above inflation are justified and this could be supported with collective action organised by their Unions.

Risk management maturity

There has been a significant growth in partnering supported by the new British Standard for Partnering, BS11000 which provides accreditation for partnerships[34] but these are frequently overlays to traditional client/ contractor contracts. Whilst the Olympics demonstrated excellent performance in the use of a Delivery Partner, it is not so obvious what the 'partnership' was. The Olympic Delivery Authority's strengths primarily stemmed from a well structured, intelligent "thin client" and an expert Delivery Partner with accountability for full program

27. Heathrow's T5: History in the Making, Op Cit
28. Ibid
29. Tender Price Indicator, Gardiner & Theobald, Oct 13
30. Heathrow Airport, Mid Q Capex Report, BAA, 2010
31. Tender Price Indicator, Gardiner & Theobald, Oct 13
32. Olympics budget rises to £9.3bn, BBC, 15 Mar 07, http://news.bbc.co.uk/1/hi/6453575.stm
33. London 2012: Olympics and Paralympics £528m under budget, BBC, 19 Jul 13, http://www.bbc.co.uk/sport/0/olympics/20041426
34. BS11000 Collaborative Business Relationships, BSi, 2010

management. The Delivery Partner and suppliers were engaged through independent NEC3 contracts[35].

Clients such as Anglian Water and Network Rail have created partnerships with cited success but other long term partnerships such as the successful 16 year BP/ Lend Lease Alliance have been sold off or disbanded.

There have been no ground-breaking evolutions in contracting strategy and even NEC has had limited increased market share. Network Rail continues to utilise an ICE Contract Form.

Reports continue to be written stating that the industry is not doing enough to manage risk and truly embrace the ambitions of Latham and Egan: "*Since Sir John Egan's Task Force published its report Rethinking Construction in 1998, there has been some progress, but nowhere near enough. Few of the Egan targets have been met in full, whilst most have fallen considerably short. Where improvement has been achieved, too often the commitment to Egan's principles has been skin deep.*[36]"

The Infrastructure Risk Group which was set up in 2010 as part of the Treasury's Infrastructure UK Task force to drive increased efficiency in construction produced its recommendations for enhanced risk management in 2013: "*.. the mitigation of risks could receive significantly more focus, a simple step that could offer major benefits for the next generation of infrastructure projects.*[37]"

The IRG's recommendations cover:

- Enhanced cost & risk estimation, moving away from standard provisions to bespoke risk based assessments
- Active risk management: incentivised mitigation, efficient contingency management and greater co-operation between organisations to share in risk management
- Develop common, industry wide, methodologies and share best practice beyond company boundaries

Alongside industry specific recommendations, new Standards have been developed or refreshed[38 39 40 41]. Yet, despite this plethora of additional guidance, there is still no accreditation system for a risk management framework and it is therefore difficult to demonstrate that an organisation has a framework truly compatible with these Standards.

Without this level of benchmarking and consistency, the ability for organisations to come together and collectively manage risk efficiently, as is essential to deliver complex construction projects – whether through formal alliances and partnerships or more traditional supply chain relationships, will be dependent on the skills of the specific managers involved in the project and a bespoke tailoring of the individual organisations' approach to suit the common Programme objectives.

Framework for a new paradigm in major programme risk management

The overwhelming consideration from this Paper is that the construction climate between 2008 and 2014 has been predominantly beneficial to clients and forecast costs for long duration programmes have been able to be maintained perhaps through superlative management but more likely due to the influence of economic conditions that have enabled actual inflationary pressures to be lower than originally forecasts.

Secondly, the Paper argues that these conditions cannot be sustained indefinitely and indeed there is a growing number of indicators to suggest the tide is turning already to conditions which might be more reflective of a 1990s construction environment: an environment symbolised by a supply chain able to charge prices far greater than historic 'benchmarked' prices as used to generate budget estimates, a necessity to seek new entrants to augment the supply chain who will be keen to take the work but will not have the maturity and experience to deliver it and essential individuals and collectives in a strong position to seek additional remuneration.

The experiences of construction client organisations and their managers over the last 6 years may limit their capacity to foresee and pre-empt the changing conditions.

The prognosis is that the risk management approaches deployed over the last 6 years will not be adequate to mitigate the consequences of a change in construction climate and a new paradigm is required to truly address the likely sea change.

35. Learning Legacy, Jacobsen J, ODA, Oct 2011
36. Never waste a good crisis, Wolstenholme A, Constructing Excellence, Oct 2009
37. Managing Cost Risk & Uncertainty in Infrastructure Projects, Infrastructure Risk Group, 2013
38. ISO 31000, Risk Management – Principles & Guidelines, BS, 2009
39. BS31100, Risk Management – Code of Practice & Guidance for the implementation of BS ISO 31000, BSi, 2011
40. PD ISO/TR 31004, Risk Management – Guidance for the Implementation of ISO31000, BSi 2013
41. Risk Management, Internal Control & the Going Concern Basis of Accounting, FRC, 2013

Construction clients could treat the new conditions encountered – when they eventually become unavoidable – as change events but the forward thinking will pre-empt the scenario as Shell did so successfully in the 1970s with the price of oil[42] and perhaps secure a similar market advantage.

The considerations that T5 went through in the 1990s might be far more appropriate to review in this scenario and if they are, then the conclusions that that programme came to and the risk management strategies it deployed – combined with more recent thinking might be would be equally pertinent. For example:

- Acceptance that clients ultimately carry all of the risk and only transfer some aspects of liability for some forms of impact at a defined cost for a limited period;
- Doing something radically different ("changing the game"[43]) when engaging the parties to a programme will generate a less complacent team, less reliant on historic mitigation strategies and more risk aware. This would reflect T5's Agreement and BS11000 by engaging the team under the full concepts of partnering rather than overlaying it on standard contracts. An innovative step would be to expand this partnering to more than just the delivery team and include key stakeholders such as the end user(s);
- Ensuring the Client has full visibility and ability to influence contingency expenditure and continuously corroborate that it is being spent on true risk rather than change or inefficiencies. A new approach to establishing contingencies associated with risk impact rather than the current Mean/ P50/ P80 slices in common use might have significant advantages as most teams now know how to manipulate this standard method to their advantage;
- Developing efficient, holistic insurance programmes with insurers actively involved in reviewing a Programme's risk promotes enhanced cross-party risk management and reduces frictional costs – or delays – which are not directly attributable to the event itself. Insurance adds no value when it is a latent cost recovery safety net post-event; and
- Escalating risk management so it becomes a key tenet of the client organisation's decision making through a coordinated Programme to Enterprise process will generate greater awareness of emerging issues and ability to redirect the Programme as required to suit the evolving business.

42. Scenarios: The Art of Strategic Conversation, Kees van der Heijden, Wiley, 2005
43. Infrastructure Risk Group, op cit

Case study 3:
Total Place - whole systems leadership

David Welbourn

The research for this case study was conducted by Prof D Welbourn in 2013, as part of a leadership study commissioned by the Virtual Staff College[1]. We are grateful to both the Virtual Staff College and the Metropolitan Borough of Bradford for permission to reproduce the case study here.

Introduction

Total Place[2] was a public sector programme in the UK, sponsored jointly in 2009 by the Department of Community and Local Government and HM Treasury. This initiative supported 13 pilot communities to generate greater public value by combining the total public budget from all the different departments serving that community. The aim was to stimulate new ways of working together to achieve better outcomes for individual service users and the wider community at a reduced total cost. Each of the pilot communities was encouraged to identify a particular aspect where the different agencies were struggling to create an effective response to the needs of the community.

Total Place in Bradford

The Metropolitan Borough of Bradford was one of these pilot communities. They focused on three distinct user groups sharing a common theme that each was in transition from one service domain into another. The potential to improve outcomes for individuals and the cost effectiveness of services is especially high in this area where users traditionally experience poor continuity and lack of co-ordination. The three transition points chosen were:

- looked-after children leaving care;
- discharge from acute hospital services of elderly patients with mental health problems;
- adult offenders leaving prison.

For each of these groups, the programme team organised a series of large-scale intense workshops designed to establish a shared understanding of how the transition was experienced by service users. This process was invariably a revelation to the provider agencies who had historically viewed the services only from their own narrow perspective. As providers heard the distress caused by dysfunctional interfaces their experience was unexpectedly, but profoundly emotional. Specific examples that emerged were used to challenge a number of myths, change priorities and create a more empathetic approach to users' needs.

Motivation for this particular pilot combined the two elements of the "burning platform" (acknowledgement that the status quo is no longer tenable), with the "burning ambition" (recognition that a more powerful aspiration was indeed desirable and achievable). This combination provided both the compelling reason to change, and the uniting purpose to motivate a rapid mobilisation towards this shared vision.

Nationally, the burning platform came from Whitehall's need to reduce overall public sector spending as part of the austerity drive in the aftermath of the collapse of the global banking sector. This pressure for change was transferred to the Local Authority through the reality of substantial budget cuts imposed on them. It was reinforced by the realpolitik that Whitehall would experience considerable difficulty of achieving the scale of budget reductions demanded, if each department was allowed to follow the usual path of defending its own preferred programmes. By transferring the problem to local authorities, whilst promoting new opportunities for intelligent, cross-departmental action, the Government hoped to reduce the impact of opposition to its actions ahead of the approaching General Election.

Whilst the financial crisis provided the focus for the burning platform, the choice of approach adopted enabled it to be promoted to emphasise the intention of improving service-outcomes, despite the austerity budgets. This paved the way for the pilot communities to warm up their ambition, but was generally insufficient to ignite into truly burning ambition. Bradford was chosen as one of the pilots because it already had a

strong approach to working in partnership together. Bradford seized the opportunity provided by this programme to foster a whole new level of commitment to partnerships that was genuinely able to ignite the burning ambition. By concentrating on the impact that poorly aligned services were having on users, they were able to find new ways of co-ordinating support and achieve significantly improved outcomes.

In July 2010 Grint[3] published his final research report on the Total Place programme overall, noting that the result of mapping local expenditure across services drew attention to the considerable sums spent on a small number of recipients. As these sums were dispersed across multiple services, there had been little historical visibility or realisation that much of this funding is channelled into repairing rather than preventing social problems. Working in isolation, each service team addressed their share of the problems as tame rather than wicked rendering their attempts to fix them unsuccessful. Grint pointed to the mistaken belief that the problems could be owned by the respective agencies involved – each of the agencies could only treat their share of the symptoms, without getting to the root problem. In contrast, the Total Place approach recognised that the real problem was only fully experienced by the individuals concerned, so only they could own its satisfactory resolution if they were placed centrally in the improvement process.

The final report from the Bradford pilot[4] identified the potential to achieve substantial savings from each of the three sub-theme areas. In each case, the savings were clearly attributed to the implementation of a care model in which all service areas shared responsibility for the whole life outcomes of the user, rather than defining those individual outcomes that could be bounded by their respective service areas. The process of working together at depth to map out the consequences for the individual enabled the different services to contribute to a joined-up intervention able to address the cause, rather than the symptoms. By moving the intervention upstream, it was often possible to suppress the emergence of much of the problem complexity faced by the service user.

This is better illustrated by an example – in this case that of young people leaving care. The whole system view developed in the joint workshops showed clearly that raising the attainment levels of those in care would create savings against the Job Seekers' Allowance budget, reduce the long term unemployment costs throughout the system and generate additional tax revenues from future employment. Additional investment in training, housing, job development and support personnel would be required to achieve this change. Similar maps of potential improvements in outcomes, cost and benefit profiles are reported for the other strands. Analysis showed that the savings rarely occurred in the same budget-line as that in which investment was needed.

The work with individual young people at the transition point helped to identify ways of providing support that led to increased self-worth and motivation, in turn contributing to raising achievement levels. In particular, the process of engagement has created a changed understanding of priorities at a detailed level. In some instances, hearing the views of those impacted by services demonstrated fundamental errors in policy thinking. One historical view that was overturned by this approach was the belief that young people should not be placed in bed and breakfast (B&B) accommodation. Although Bradford only had few cases where youngsters were in B&B, this was becoming a significant political issue for the Council. By engaging with those affected, it transpired that living in B&B might be the preferred option in those cases where individuals still sought the experience of living in a family home with the support and often encouragement of the owners. For some, such a supportive family environment could be significantly less daunting than the challenges and responsibility that full independence demanded from those placed in a hostel without an effective network.

Despite its short life, the programme was successful in identifying the potential to combine financial savings with better outcomes. It is abundantly clear from those interviewed that the local successes have been achieved by building a compelling purpose – a golden thread – around the inspiration of achieving better outcomes for individuals. So, for example, the probation service has continued to invest in providing support in the golden 24 hours after discharge, even for those for whom the probation service has no formal responsibility. Such support breaks the trend of those released falling straight back into crime, helping them to find accommodation and reintegrating back into the community. Funding for this has been found within the "discretionary" elements of the community safety partnerships budget.

Systems leadership in action

The Total Place programme was relatively short lived due to changes in policy, but for those involved it was a very intense experience. Attitudes, behaviours and relationships were different amongst those who had been involved in the service design workshops, exposed to the powerful narratives generated by service users, and involved in the intensity of the "deep-dive" process by which evidence was gathered and alternative, more

effective solutions were developed from the perspective of service users, rather than providers. Individual leaders describe profound experiences that led to sustained personal changes that can transcend specific initiatives. One leader described the Total Place programme as a "life-changing experience" both personal and professional, with a total commitment to a new, more inclusive way of working. "*I am not prepared to go back to the old way of working*". Others described the transformational impact of the programme in similar terms. *"It was almost as if you had been converted". "It was like immersion – you'd either been through it or you hadn't*".

It was also clear from the interviews that the problems faced by those making the greatest demands across services are wicked problems that cannot be addressed superficially or in separate service compartments. Leaders have to be committed to engaging deeply into the details, working intensively with other agencies, and listening attentively to the users' voices, with the uniting and primary purpose of achieving sustainable outcomes for individual users. The challenge for senior leaders is to model this behaviour for deep involvement in a small number of priorities at a time when growing workloads and widening portfolios reinforce models based on light-touch engagement.

Adopting a new approach to risk was a fundamental ingredient of success in this enterprise-wide approach. There was clearly an appetite and willingness amongst the partnership to see Bradford in a different light and view it through others' perspectives. For some, this was interpreted as taking risks by putting other organisations' ahead of self-interest, but this was equally described as a willingness to cede power and authority to other partners for the greater good. Others talked more of boldness and courage to challenge each other, ensure matters were placed openly on the table and confronted in order to make progress. Signs of willingness to take risks were often shared by those interviewed in the course of normal conversation about the services. So, for example, the probation service has learnt sufficiently from the experience of drawing offenders into service design, that one has been employed as part of the permanent team – a remarkable level of risk for a service traditionally associated with conservatism. In another example, the housing providers were commissioned to make provision for young people leaving care to be housed in decent accommodation alongside good neighbours, rather than the conventional assumptions that treated them as probable trouble-makers who were best housed in more disadvantaged neighbourhoods.

A key message from these illustrations is that it is necessary to break the stereotypes that hold people back. In both these instances, it also means ignoring the pareto principle of focusing on the mainstream. The small numbers of special cases cannot be ignored in favour of the majority – in a world of complexity, it is those on the margin who will prove to be more significant over the long term (clearly demonstrated in the financial cases made by Bradford).

The case study also reflects another important change to leadership practice when working at the whole-system or extended enterprise level. An important element of the success arises when leaders are willing to engage personally at an unprecedented level of depth with their peers from across the system. In this case, the sheer number and size of the workshops and the depth of detail they required made substantial demands on senior leaders. The energy generated through this process and the emerging sense of purpose combined to encourage the most senior leaders to sustain their personal commitment, despite the traditional temptation to delegate such details lower down the organisation. The truly visionary change will only occur when the most senior (i.e. those with the broadest reach and compass) remain engaged in this way. In this instance their effort was rewarded by the personal experience of working differently as described in their feedback.

The involvement of service users and the challenging nature of some of their stories created some difficult moments of mutual blame at the beginning of the process, but these were overcome by the strength of existing relationships. Leadership across the extended enterprise is not always comfortable and this is a real example where "cooking the conflict" allow a greater sense of maturity and respect to emerge the other side.

Grint[3] describes the success of Total Place as resting in a balance between central forces initiating a new authorising environment and local forces who built momentum as they took local ownership for behaving differently on priorities defined within their specific local context. Corrigan[5] describes this as the outworking of both centripetal and centrifugal forces – natural tensions that are part of the complex order that is best illuminated by an understanding of complex adaptive systems[6].

Grint's review emphasises the systems nature of Total Place – drawing out that the programme emphasises the need to be clear about precisely what problem is being solved, establish a clear sense of purpose, and acknowledge that in this approach, the key answer does not lie in normal power relationships. But perhaps the most important element of his conclusion is that leadership is not vested in individuals and their characteristics, but distributed between many

individuals and grounded in the context of time and place, informed by the local knowledge (frequently tacit rather than explicitly shared) within that community.

The case study illustrates the importance of leadership characteristics attuned to whole systems thinking:

- the creation and sharing of a compelling common purpose, beyond the ability of any individual organisation to deliver alone;
- a process of service redesign focused on direct user experience and involving all service agencies creates a substantial movement for change that is able to achieve better outcomes and provide evidence to debunk a number of myths;
- the fresh insight and transformational approaches developed has been described as life-changing by some leaders;
- when leaders experience the benefits of working across whole systems, their personal attitude and approach to leadership can be changed sustainable change extending significantly beyond the pilot programme;
- systems leadership has a disproportionately beneficial impact on a small number of users who usually fall below the radar in traditional "pareto-based" approaches because they sit at the heart of multiple systems, confronted by complex and "wicked" problems;
- solutions were found to these wicked problems because senior leaders were willing to engage personally at a deeper level, building stronger relationships and a greater understanding – system leadership depends on a richness of both information and skills in analysis/ synthesis;
- the tensions that are inherent to wicked problems are an important source of energy ("cooking the conflict") leading to better solutions if confronted openly;
- leaders exhibited courage in adopting new approaches and were able to achieve greater outcomes through their willingness to cede power to others;
- the demands and relevant styles of leadership that contribute to effective outcomes across the extended enterprise will be shaped by the context – both time and place.

References

1. Systems Leadership: exceptional leadership for exceptional times –Source paper 3 – UK leadership scenarios, Jane Lewis, David Welbourn, Deborah Ghate, Virtual Staff College, October 2013 http://www.virtualstaffcollege.co.uk/wp-content/uploads/leadership_scenarios_complete.pdf
2. HM Treasury: Total place: a whole area approach to public services. (2010).
3. Keith Grint: Problem, purpose, power, knowledge, time and space: Total place final research report. Local government leadership (2010).
4. Bradford_Metropolitan_Council Bradford District Partnership Total Place Final Report. (2010).
5. Paul Corrigan, private conversations and see for instance http://healthycommunities.kindofdigital.com/2011/11/a-national-perspective-paul-corrigan/
6. Chapter 3 of this document: Leadership, management and Governance

Goodbye Spreadsheets, Hello Cloud

Managing the governance, risk and compliance (GRC) needs of an organisation is becoming increasingly challenging. Inadequate GRC processes can lead to non-compliance with regulatory standards and result in severe financial penalties, brand damage and even imprisonment.

The SureCloud ® Platform provides an agile, cost effective approach to GRC process automation, is fast to deploy, and minimises business change – providing the central control, visibility and efficacy that is missing from spreadsheet-based approaches.

Automate existing administrative processes with SureCloud ® and escape the inefficiencies of labour-intensive spreadsheets.

CONTACT US FOR A PLATFORM DEMO

- Business Continuity Management
- Compliance Management
- Incident Management
- Issue Management
- Policy Management
- Risk Management
- Third Party Management

SureCloud®

www.surecloud.com
Tel: +44(0)118 963 7999
info@surecloud.com

IRM
T: +44(0) 20 7709 9898
E: enquiries@theirm.org
W: www.theirm.org

Sackville House
142-149 Fenchurch Street
London
EC3M 6BN

SureCloud
Richard Hibbert
Chief Executive Officer
richard.hibbert@surecloud.com