Institute of Risk Management

Extended Enterprise:

Managing risk in complex 21st century organisations

Executive Summary

SureCloud

irm

Our supporters

Contents

IRM is the leading professional body for risk management. We are an independent, not-for-profit organisation that champions excellence in managing risk to improve organisational performance.

We do this by providing internationally recognised qualifications and training, publishing research and guidance and raising professional standards across the world. Our members work in all industries, in all risk disciplines and across the public, private and not-for-profit sectors.

Foreword

Extended enterprise is about far more than 'supply chain risk management.'

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 are 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. Recent examples of why we should be concerned about this include the scandal in the UK when horsemeat appeared in some beef supply chains; the management by some banks of their outsourced IT providers and the tangle of responsibilities that became evident following the Macondo well disaster in the Gulf of Mexico.

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. 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.

As well as supporting organisational performance, a better understanding of extended enterprise is also vital if we are to play our part in tackling wider problems including slavery, abuse, environmental damage and dangerous working conditions. Wilful blindness by organisations to these issues within their extended enterprise is unacceptable.

This short document summarises the work undertaken by a project group of IRM members and subject experts over 18 months. It is relevant for all professionals, particularly those working at board level, and we finish by offering a set of questions that we think all boards, assisted by their risk professionals, should be asking about risk in their own extended enterprises.

The group has also prepared a comprehensive 'Resources for Practitioners' document, providing detailed insights into many of the topics covered in this summary. This document is available to IRM members and to the members of our supporting organisations, to download from our respective websites.

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 on what we have done.

> Management of risk in the value chain can only ever be as effective as the management of the weakest link in it.

Boards will need to do things in different ways – leading rather than managing.

I am grateful to the members of the project group (who are all named at the end of this document) for their dedication to this work. 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.

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.

Boards are facing new challenges in managing risk in this world of complexity and extended enterprises. They will need to do things in different ways – leading rather than managing and building collaborative relationships based on values and communication rather than focusing on process. We hope that this work provides some encouragement to start on this path.

Richard Anderson, Chairman
Institute of Risk Management

What do we mean by extended enterprise?

No organisation today has direct control over every aspect of its operations or reputation.

Our definition: An **extended enterprise** is a structure where a number of organisations come together in a joint endeavour in order to achieve outcomes that none of them could have achieved on their own.

What extended enterprises do you rely upon? And which rely on you?

The past decades have seen a transformation in the way that both private and public organisations operate. Delivering a product, a project or service today is likely to involve multi-tiered, often global value chains, sub-contracted manufacturing, licensed intellectual property, outsourced back offices and complicated routes to market, including digital delivery, all under increased pressures of time. In the public sector many governments are handing over service delivery to a network of private or third sector operators.

By collaborating and specialising we can achieve outcomes that individual organisations could never achieve on their own. But it also means that no organisation today has direct control over every aspect of its operations or reputation – from the smallest start-up purchasing web and IT support from a cloud-based supplier to the complex supply chains of the largest supermarkets. Risk management for these vital, complex extended enterprises that we rely on so much in our modern economies may be uncoordinated or inadequate.

Up to 80% of operating costs today may originate from outside the organisation.[1] Intangible assets including goodwill have become increasingly important in assessing the value of companies. As the amount of physical assets owned directly has decreased, so the performance of extended enterprises in delivering that intangible value becomes more significant. New information and communications technologies have facilitated the expansion of extended enterprises but have also introduced new risks that must be understood, considered and managed.[2]

1. Source: Institute of Collaborative Working 2014.
2. For more detail see www.theirm.org/knowledge-and-resources/thought-leadership/cyber-risk/

…we are starting to explore the less predictable behavioural and cultural issues driving organisational performance.

From enterprise risk management to extended enterprise risk management

The development of the discipline of risk management in recent years saw practitioners understandably starting close to home – by looking at what could be done within a single organisation. They began by bringing together individual activities associated with managing risk into a coherent enterprise risk management programme. We now have a broad body of knowledge about the processes that should be in place and the frameworks and architecture necessary to achieve this. ISO 31000, for example, sets out a systematic approach for identifying, analysing, evaluating and treating risk.

Notably, the first step in the ISO 31000 process is establishing the context. And it is in this area that we are starting to explore the less predictable behavioural and cultural issues driving organisational performance. IRM's 2012 publication on Risk Culture[3] started to look at this subject. It is also here, in establishing the context for risk management, that the issue of complexity and extended enterprise arises.

Understanding our extended enterprises, managing the risks of the relationships that bind them and considering how our risk management approach should be adapted to deal with them is the purpose of this project.

Disruption costs

'Japan Earthquake May Cause Prius Shortage'

'Nissan to Suspend Domestic Lines because of a delay by supplier Hitachi Ltd in delivering auto-engine components' and

'Vestas Shares Fall 20 Percent Following Production Delay Warning'

Research from Accenture indicated that announcements like these about supply disruptions led, on average, to a 7% reduction in shareholder value.

Source: Building Resilience in Supply Chains, World Economic Forum, 2013

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

A model to understand the extended enterprise

Figure 1:
Joint Endeavour

Multiple Economies in Diverse Societies

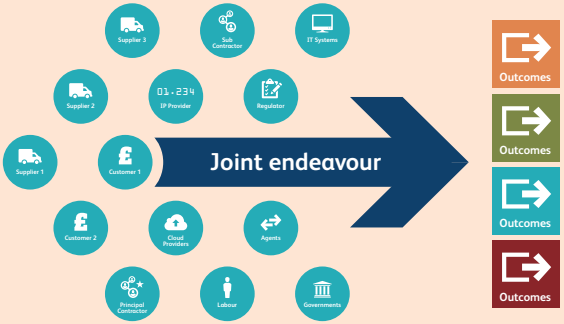
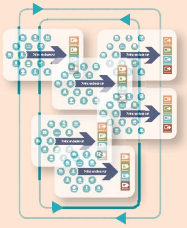


Figure 2:
Further Interconnections

Multiple Economies in Diverse Societies



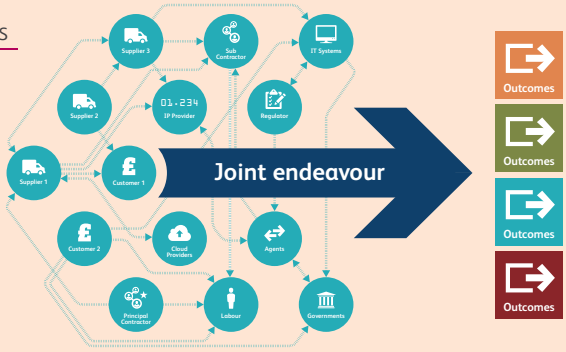
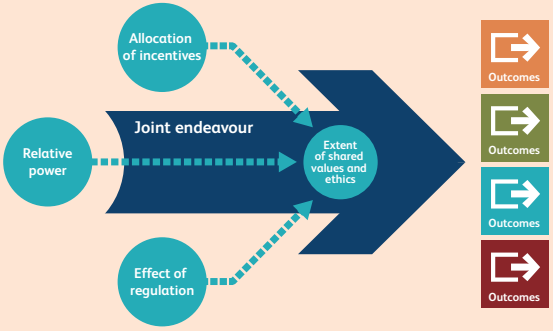


Figure 3:
Key Dynamics

Multiple Economies in Diverse Societies



> …alongside the risks, there is also significant potential for strong parts of the network to deliver benefits and opportunities.

Our project group has developed a number of models, tools and techniques to help understand and manage risk across our extended enterprises. Our way of looking at how extended enterprises come together is as follows and is illustrated diagrammatically on the left.

Figure 1: Joint endeavour
Against a background of multiple economies in diverse societies many people and organisations will work together on a joint endeavour to achieve outcomes. These could include manufacturing or distributing products, delivering public services like healthcare, education or defence, or achieving a large or small infrastructure or scientific project. The network that comes together to achieve this includes not just direct suppliers and customers but will also have links to other parties, including regulators and the media, as well as a multiple-tiered supply chain.

Figure 2: Further interconnections
The picture is further complicated by other connections between the parties, for example within an industry sector, which could be either collaborative or competitive, and by all parties' involvement in further multiple joint endeavours.

Some parts of this joint endeavour will have good risk management within their organisation, others less so. But uncertainty multiplies within this web of complexity, with serious potential for 'weak links' to affect other parts of the network. More positively, alongside the risks, there is also significant potential for strong parts of the network to deliver benefits and opportunities for all in areas such as innovation. The important subject of innovation within extended enterprise networks is covered in detail in Chapter 7 of our longer companion document.

Figure 3: Key dynamics
The likelihood of achieving the desired outcome for the joint endeavour will depend on the following four key dynamics:

- the relative *power* of the participants
- the *incentives*, monetary and otherwise
- relevant government or other *regulations*
- whether there is a sense of shared *values and ethics* across the joint endeavour.

A more detailed account of our thinking is included in Chapter 1 of our companion 'Resources for Professionals' document.

Complex 21st Century Organisations

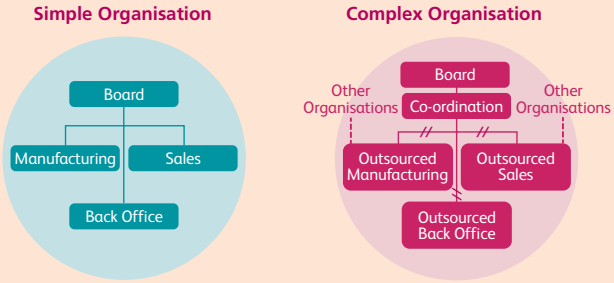
In the world of the extended enterprise the role of the board has to change from one of 'command and control' to one of leadership, co-ordination and influence.

It quickly became apparent during our work that the environments analysed and the risk management problems they present, display many of the characteristics of complex systems. A complex system, like the weather, is one where even if you know everything there is to know about the system it is not sufficient to predict precisely what will happen, although it is possible to discern a range of outcomes. When simple systems are put under stress they can start displaying many of the attributes of complex systems.

Simple or Complex?

Simple Problems	Complex Problems
Usually structured – similar issues encountered	Unstructured and unfamiliar
Easy to control and predictable	Hard to control, unpredictable
Deterministic: if you do the right things there will be a predictable outcome	Adaptive: new and unexpected problems will arise as you try to take action
Normally susceptible to a single professional discipline	Require multiple disciplines working together in new ways
Information to solve the problem is easily available	Vast amounts of information may be available but defy easy organisation and analysis
Can be managed consistently by rules and processes	Must be managed creatively by means of principles, shared ethical values and behaviours

Figure 4: Simple and complex organisations



When a system is complex, it can achieve increased efficiency and performance, as well as increased capacity to adapt to its external environment. Unfortunately, these systems are also more sensitive to instabilities (sometimes catastrophic) and rather fragile when central elements are affected, especially multiple events in a short timescale. This can lead to cascades of failure, for example:

- A fragile economy that is 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 at many levels, ranging from economic to environmental.

Governance in complex organisations

In a simple organisation, as seen in the diagram at Figure 4, the board directly controls manufacturing, sales and the back office. Communicating instructions and feedback also fall directly within the same span of control. In the complex organisation, or extended enterprise, manufacturing, sales and back office may now be outsourced to third parties. Many brand-based organisations operate in this way, and it is common for banks and other financial institutions to outsource many aspects of their businesses.

The difficulty this creates for risk management is that it breaks the communication lines. Those who 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. The different components may operate in different geographical and regulatory environments and have different risk cultures, risk appetites and tolerances. In extended enterprises the role of the board must change from one of 'command and control' to one of leadership, co-ordination and influence. Relationship management and collaborative working across the extended enterprise become essential. Boards need to develop a clear understanding of their extended enterprise. This includes an appreciation of the relative power, incentives, motivations, culture and ethics and operating conditions of the key participants.

Power, motivation and cat litter

Chrysler found out just in time that important castings for the engine of its market leading Grand Cherokee jeep were ultimately dependent on a small niche supplier of casting clay ceramics. The supplier had been managed down to such an unprofitable position by the power of its customer that they were considering producing cat litter instead. Had Chrysler not found out and addressed the situation in time, this could have been disastrous for them

Source: Clockspeed by Charles Fine. Perseus Books. 1998

Modelling the extended enterprise

Modelling your extended enterprise helps identify the ultimate location of risk across the network.

We have worked with network modelling experts to advise us how to map the complex extended enterprise. Complex networks provide a powerful modelling framework which has been successfully applied in a range of real world complex systems, from the human brain to shipping routes and the economy.

Why would we want to model our extended enterprise?

Modelling your extended enterprise helps identify the ultimate location of risk across the network. It benefits the organisation by:

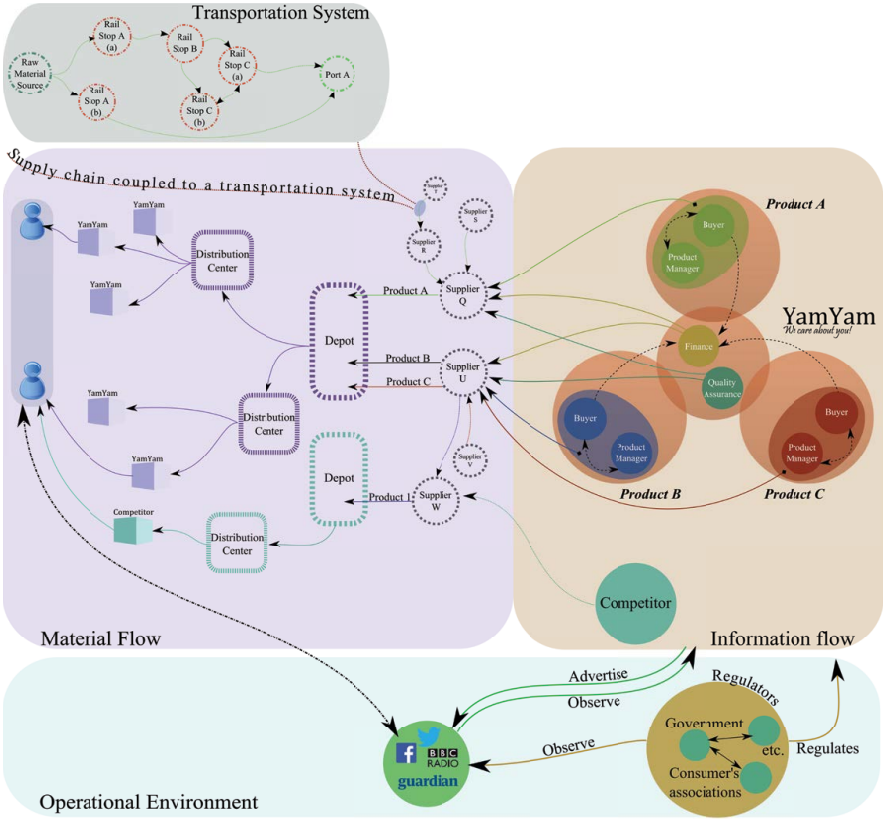
- gaining a detailed understanding of the value chain through the system to help improve performance and efficiency
- identifying key points in the network which control flows of information, physical goods or money so that risk and audit attention can be focused on these areas
- helping to identify what can be controlled, what can be influenced and what can only be monitored
- building resilience by identifying where links are weak, undervalued or missing
- allowing scenario planning and stress testing by analysing the effects of taking out elements or sections and disrupting flows
- improving the ability to be able to respond to external and internal shocks by understanding in advance what the effects might be
- improving response times and reducing disruption costs when dealing with an incident
- providing a framework for looking at the key dynamics of power, incentives, regulation and values and ethics.

How is it done?

Our longer companion document contains a detailed account of how to apply network analysis techniques to an extended enterprise. In summary, you should first decide on the boundary of your extended enterprise. This involves deciding what to include and not to include, based on the degree of control and influence that various entities could exert within the network. You can then start to map the enterprise, thinking about how the various entities are connected. This could be by flows of physical goods, information, money, regulatory control or social interaction. The process is of course iterative, as analysis informs judgement on what should be included.

Figure 5 shows the sort of network map that might emerge from an analysis of the fictional organisation 'Yam Yam', identifying the key entities – '*nodes*' – in the network and the connections between them.

Figure 5: Example diagram of a mapped extended enterprise



You should first decide on the boundary of your extended enterprise.

Network analysis

Once the network is mapped, you can start applying network analysis techniques at a global (network) and local (node) level. This helps us think about real life organisations and relationships, trading partners and flows of goods, finance or information in a systematic way and can include:

Analysing the nodes:

- **Degree centrality** – how many neighbours does each individual node have
- **Closeness centrality –** how easily a node can reach any other node, i.e. how close it is to its neighbours in terms of hops. Nodes requiring lots of hops to reach are clearly more difficult to control
- **Betweenness centrality –** how important any node is in connecting other nodes – this is a measure of control of flows through the network and can indicate potential bottlenecks
- **Neighbours' characteristics –** how important, central or influential a node's neighbours are. This idea is used by internet search engines – it can identify apparently unimportant nodes with low connectivity which nevertheless could have a big impact on a more important node.

Analysing the network:

- **Network distribution –** the degree to which the network is homogeneous (with every node having more or less the same number of connections) or heterogeneous (with most nodes having very few connections with the occasional super-connected node). There are important implications here in terms of network resilience
- **Network density –** the extent to which the network uses all its possible connections. Highly connected networks may mean that individual nodes are less important, yet shock waves will spread widely and quickly through the system
- **Network complexity –** a measure driven by both distribution and density. It includes the additional effort and resources that denser networks and highly connected nodes need to operate and takes us further into the realm of unpredictable complex systems.

Chapter 2 of our companion document 'Resources for Practitioners' includes a detailed account of how network analysis might be undertaken.'

Leadership, management and governance

A complex system cannot be controlled. However it can be influenced.

Whilst stronger control may improve performance in simple systems, this is not true in complex systems. A complex system cannot be controlled. However it can be influenced. And the more the system is able to adapt and learn, the greater the probability that it can be influenced or nudged into the desired state. Traditional understanding of governance and risk management has been dominated by process thinking, but in the extended enterprise we need to give at least as much attention to relationships, attitudes and behaviour.

More rules, regulations and contracts are never the full answer for complex problems and can actually be counterproductive. A regime focused on enforcing compliance stifles any sense of ownership, constrains the initiative of individuals and teams and suppresses innovation and improvement – the very elements that fuel sustained success. Enquiries into both the banking collapse and failures of safeguarding for children in care have both concluded that improvement does not come from more procedures and tighter compliance but from addressing leadership, cultural and behavioural issues.

Our leadership model for the complex extended enterprise builds on a clear and authentic vision and values and takes advantage of curiosity to build trust and demonstrate courage in actions and behaviours. The model is shown diagrammatically in Figure 6 and its essential elements are:

Be clear

In the world of the extended enterprise, the foundations for success are built on a compelling vision, clearly expressed, and on the alignment of explicit values that are constantly reinforced by the way that leaders demonstrate them in practice. The more powerful and attractive the vision, the more likely it is that followers will buy that vision and commit their personal energies to achieving it. But it must be sincere, sustained and aligned to motivations and values to succeed in the long term.

Be curious

Successful leaders of complex systems show a heightened sense of curiosity that simultaneously seeks new knowledge and new relationships from as many different contexts as possible. This helps create the learning, questioning and adapting system that can be guided to support the vision.

> More rules and regulations are never the full answer for complex problems and can actually be counterproductive.

Be courageous

The final tier of system leadership is therefore characterised by courage – the courage to rewrite the rule book in terms of personal behaviours, risk taking and the ability to face paradox and uncertainty by relying on others and working constructively with the energy of conflict.

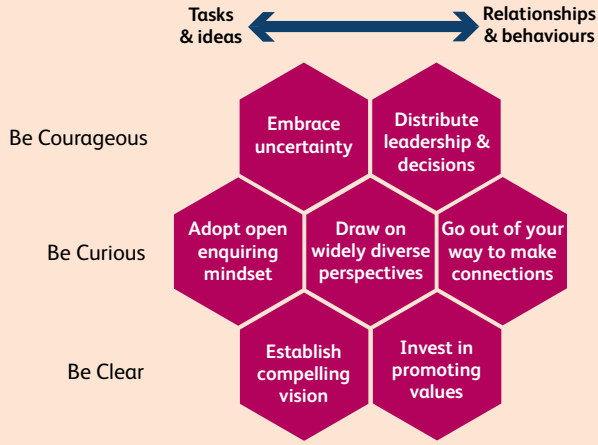
Good governance cannot be imposed through compliance with standards but needs to be constantly revised and improved. This involves balancing good processes with wise judgement in a constant renewal process built on valuing diversity, developing self awareness and regular benchmarking.

Seven characteristics of people who are successful in leading complex organisations

- they go out of their way to make new connections
- they adopt an open, enquiring mindset, refusing to be constrained by current horizons
- they embrace uncertainty and are positive about change – adopt an entrepreneurial attitude
- they draw on as many different perspectives as possible; diversity is not optional
- they ensure leadership and decision-making are distributed throughout all levels and functions
- they establish a compelling vision which is shared by all partners in the whole system
- they promote the importance of ethics and values and invest as much energy into relationships and behaviours as into delivering tasks.

Risk professionals who want to operate successfully in the extended enterprise will need to develop a range of capabilities including dealing with paradox and ambiguity, managing conflict, collaborative working, stakeholder engagement, risk communication and future scanning. Our longer companion document gives a more detailed account both of leadership and governance (Chapter 3) and also of the capabilities required of risk professionals (Chapter 9).

Figure 6: Desired characteristics for whole system leadership



CASE STUDY

TOTAL PLACE

Total Place was a public sector programme in the UK between 2009 and 2011. It supported 13 community initiatives which encouraged collaboration between multiple agencies to achieve better outcomes for individual service users and the wider community at a reduced total cost. Typical problems included childrens' services, adult offenders leaving prison and elderly patients with mental health problems being discharged from acute hospital services. The new approach showcased many characteristics of whole system leadership. This included a strong vision focusing on the personal experience of service users, changes in service providers' behaviour as they were empowered to act in the interest of the user, rather than their immediate organisation, and a deep understanding of the motivations and connections between all involved.

Ethics and behaviour

Behaviour, ethics and values are an essential element.

> *"Business is about people, a complete ecosystem where all things are connected to each other. The human dimension is essential when assessing, communicating, managing and advising upon risk. The real world is about people and politics."*
>
> **Anthony Hilton**
> Financial Editor of the London Evening Standard, speaking at an IRM event in 2012

As we have seen, complex systems cannot be effectively controlled purely by means of systems and processes but require the alignment of explicit values that are constantly reinforced by the actions and behaviours of leaders. In IRM's previous work on risk culture[4] we argued for a better understanding of the drivers of ethical behaviour and the importance of these factors in determining the risk culture of an organisation. These principles carry forward into the extended enterprise: behaviour, ethics and values are an essential element in understanding and managing risk. Chapter 6 of our longer companion document gives more detail of an approach to understanding ethics in this context.

CASE STUDY

DE BEERS

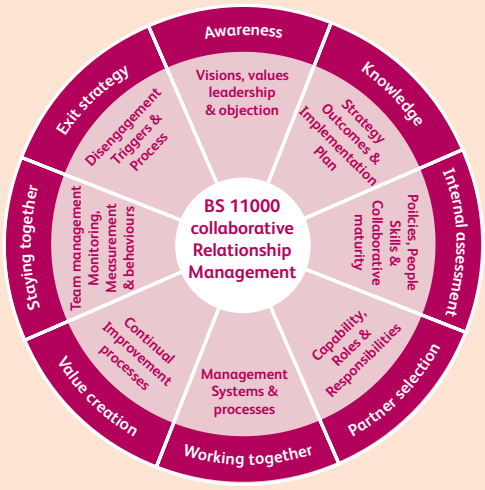
Multinational diamond trading business De Beers maintains a set of Best Practice Principles – a mandatory code of ethical business conduct supported by an assurance programme. The principles apply to every employee at every level within the De Beers family of companies, joint venture partners, contractors and Sightholders (customers purchasing rough diamonds for resale). Almost a quarter of a million people worldwide are covered by the Best Practice Principles which cover issues such as child labour, conflict diamonds, environmental damage and working conditions.

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

Building collaborative relationships

In the world of the extended enterprise, whether in the public, private or third sector, the risk of breakdown of relationships with customers, partners and suppliers deserves a higher profile. Increased outsourcing and use of external contractors tends to lead to a greater emphasis on the scope and rigour of contracts. The aim is to transfer risk and responsibility to the greatest extent and rely on the contract to allocate liability in the event of a break down. This approach can in itself be risky as the contract can only provide the financial and performance framework. It is unlikely to be able to influence integrated performance or softer but equally important aspects such as maintaining visions and values, culture, ethos and commitment. And it is the culture and values of an organisation that really drive excellent performance, not regulations and measures. We believe that this approach can also be helpful for looking at how the internal relationships in large organisations work as well as the external ones.

Figure 7: Collaborative Relationship Management



The BS 11000 Collaborative Business Relationships series[5] provides some guidance on a systematic approach to managing the risks and opportunities of relationships in both the public and private sector. It is summarised in Figure 7. The backbone of the framework is a relationship management plan which sets out the organisation's approach and requirements. Key aspects which should be included are:

- A sound business case for the relationship, including measures of success
- Appropriate policies, people and skills to support collaborative working, including a partner selection process
- Operational management focused on working together and resolving conflicts
- A commitment to continual improvement and added value over time
- Day to day monitoring and management of the relationship, including joint risk management
- An exit strategy, with the risks of disengagement fully understood.

The backbone of the framework is a relationship management plan which sets out the organisation's approach and requirements.

5. For more information on this subject see www.instituteforcollaborativeworking.com

Sector collaboration

If all parties work jointly to understand and mitigate the risks, then the entire extended enterprise becomes more resilient as a result.

We believe that there is significant potential for risk leaders within industry sectors, possibly led by industry associations, to collaborate with each other to reduce overall supply risks and promote the long term health of the value chain in that sector.

This process recognises that risks can come from sources outside an organisation's own supply chain, but still within the same industry. For example, the 2011 Thai floods directly affected Seagate, a hard disc supplier but also led to a fall in orders at Intel, even though Intel was not directly connected with Seagate. Seagate's customers, however, had to scale back their production leading to a fall in demand for Intel chips. Both companies were part of an extended enterprise providing key components in the computer sector.

The key steps in building a sector level approach are:

1. Identify the extended enterprise – by mapping the sector to identify the key players
2. Identify and assess inter-company risks originating from the various types of organisation involved at the different stages in the production and distribution process, together with the impact on the 'upstream' and 'downstream' entities within the extended enterprise
3. Mitigate the risks by preventing their origination or transmission. Each organisation involved can share what it is already doing and identify areas where a collaborative solution will be beneficial.

In our longer 'Resources for Practitioners' pack we include in Chapter 14 a practical worked example of how this could operate based on the European aluminium industry.

If all parties work jointly to understand and mitigate the risks, then the entire extended enterprise becomes more resilient as a result. The longer term success of such alignment must eventually be based on shared values and ethics, as well as shared information.

Communications challenges

As enterprises become more complex and diverse, it becomes increasingly difficult to ensure common linguistic understanding and interpretation of key messages. There is also a variety of new communications styles, including social media, which are difficult to control but impossible (and unwise) to ignore. Yet the need for clarity of communication becomes even more important: without it there is unlikely to be a uniform purpose, shared beliefs and ethics or a means to achieve assurance for all stakeholders.

Mapping the enterprise should help identify those that need to be communicated with and also key points where failure could be a problem. It should also highlight differences in culture and environment that might affect perceptions of risk although finding common ethical ground in extended enterprises dominated by cost issues may be a challenge. A pro-active risk communications plan, including specific plans for incident response, should be an essential element of an extended enterprise risk programme. This subject is developed further in Chapter 10 of our longer companion document.

A pro-active risk communications plan, including specific plans for incident response, should be an essential element of an extended enterprise risk programme.

Assurance challenges

Automation which makes use of technological solutions may be the key to delivering such capabilities in some organisations.

Assurance helps executives and boards to sleep at night. It aims to give confidence, possibly backed up by proven compliance with published standards, that what you are told is happening, is actually happening. It may be provided by independent third parties, or by independent internal functions such as risk management or internal audit, and should be based on a review of processes, systems and controls. But how far can we take this process in an extended enterprise, where we know that a failure in one organisation can impinge disastrously on another?

Extending assurance processes beyond the boundaries of the organisation presents us with some problems:

- In some areas (e.g. IT security reviews) it can appear that everyone is auditing everyone else. This happens as organisations seek assurance about their suppliers, and sometimes (usually following a problem) their suppliers' suppliers, leading to confusion and expensive duplicated effort
- There is a danger that the enterprise can become tied up in a web of overlapping and possibly conflicting standards
- Not surprisingly, some organisations show little interest or capability in seeking any assurance beyond their own boundaries.

A first step

Direct supplier/partner relationships need a system of assurance that reflects the organisation's risk profile. The assurance process should be structured (consistent and repeatable) agile and efficient. Automation which makes use of technological solutions may be the key to delivering such capabilities in some organisations. However other important elements include adopting a risk-based approach for categorising suppliers, ensuring that contracts give the organisation the right to audit and managing the relationship effectively.

Reaching outwards

Taking this outward into an extended enterprise, we believe that three elements need to be in place for the boards of the organisations involved to begin to gain assurance:

1. An agreed form of *governance* that works across the extended enterprise that understands the four key dynamics of power, incentives, regulation and values and ethics

Assurance across the extended enterprise will need to be more relationship based.

2. An understanding of risk management *capability*, which in our guidance on risk appetite and tolerance[6] we defined as a function of capacity (how much risk can you carry?) and maturity (how well can your people cope?)

3. A flow of appropriate risk management *data* between organisations, particularly data relating to forward looking key risk indicators.

We think that assurance across the extended enterprise will need to be more relationship based, more forward looking and will involve conversations in risk between all parties. There is a need for a general up-skilling of risk management and assurance across the enterprise to achieve this and for the development of new tools and techniques to help. We provide further analysis in Chapter 11 of our longer companion document. Further information on the role of internal audit in shared and outsourced services can be obtained from the Institute of Internal Audit.[7]

A future assurance model?

As a more radical option, we suggest that industries could collaborate to develop Assurance Clearing Houses. These would allow all participants in multiple extended enterprises to gain a single assurance certification rather than multiple certifications.

6. www.theirm.org/knowledge-and-resources/thought-leadership/risk-appetite-and-tolerance/
7. www.iia.org.uk/buy-iia-technical-guidance/

Questions you should be asking

- How complex is our business operating model? How extended is our enterprise? Have we analysed it?
- What additional risks does complexity pose and how do we manage them?
- Which key components, processes, functions or people could, if they fail, stop us operating?
- What scenarios could trigger a systemic reaction that could cause widespread damage?
- Have we thought about the social dynamics (power, rewards, regulation and shared ethical values) across our extended enterprises? Do we understand what motivates other key participants and how they will behave under stress?
- Have we thought about the risk appetite and tolerance of members of the extended enterprise and how these compare to our own?
- Have we thought about the risk culture of other participants and how it compares to our own?
- Do we set an example of ethical, decent and right-minded behaviour in order to build trust and foster these behaviours through the enterprise?
- Do any claims that we make about our organisational values hold true across our extended enterprise?
- How do we satisfy ourselves that we know what is going on throughout our extended enterprise? How do we get helpful risk information?
- Are appropriate governance structures in place to ensure that the likelihood of success in the joint endeavour is maximised?
- Has the board devoted sufficient resources to creating and maintaining an adequate risk management and assurance framework that functions across its extended enterprise?
- Do our senior people have the right skills and capabilities to lead a complex extended enterprise?
- Does our extended enterprise structure support or stifle innovation?
- Do we give sufficient consideration to the risks associated with our relationships? Is there a senior executive responsible for relationship management?
- Do we understand how communications flow through the extended enterprise, how perceptions may vary and how this affects risk management?
- Do we understand our reliance on outsourced IT and cloud based services and the risks that these may bring to the enterprise?

Our project team

IRM would like to thank our own extended enterprise which has come together to draft and review this guidance:

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 Afflilate, 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.

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 9808
E: enquries@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