Managing Risk and Resilience in the Supply Chain

David Kaye
FCII, FBCI, FRSA, MIRM
# Contents

*Introduction*  
1. Risk management and modern day business models  
2. Risk management, supply chain management and bringing the two together as supply chain risk management  
3. The special risk features of the supply chain project  
4. Risk managing a supply chain dependency or dependencies  
5. Dependencies outsourced  
6. Myths and realities  
7. Business continuity – both a science and an art  
8. Third-party relationship management  
9. Benchmarking and gaining of confidence  

*Appendix 1. BS and ISO standards*  
*Appendix 2. Selection of corporate governance and trade compliance requirements*  
*Appendix 3. Examples of other standards*  
*Further reading*  
*Index*
Introduction

Risk managers understand that the consequences of damage by an unexpected incident may be measured in more than simply financial terms. There are more ways, and potentially much more destructive ways, of a risk incident harming an organization and its people than the loss of assets, revenues and cash flows, or the financial cost of litigation. The most destructive of impacts from a risk incident can be to render the organization unable to deliver on current contracts and continue to meet its responsibilities to stakeholders. A risk incident can also destroy an organization’s ability to manage and retain control, and remain legal and compliant.

The impact may enforce a period of time when the organization cannot remain an effective player in its ‘market-place’. It does not take long for that displacement to destroy brand values and other confidences or for competitors to rush in and wreak long-term damage to the organization’s customer base and other important stakeholder dependencies. Even when the organization is a monopoly or public service supplier, the way stakeholders and customers react to a real or perceived fall in service levels can turn a hiccup into a disaster.

The risk manager must therefore ensure that all of the operational dependencies and tools necessary for the organization’s survival remain accessible quickly enough to be of use. These dependencies are much more than money and assets. They include, crucially, a wide range of intellectual assets, effective business controls, regulatory approvals, legality, regulatory compliance, the confidence of its various stakeholders, its brand values and its reputation. It includes of course whatever assets, tools and skills – wherever they are positioned in the value chain – an organization needs to be able to continue to deliver urgent, contracted products and services, on time and of the expected quality. Extreme financial damage from an unpleasant surprise may indeed be sufficient to divert the financial business model sufficiently to render the organization no longer viable. The non-financial impacts, however, are equally, if not more likely, to bring greater damage or even corporate death.

The cause of that corporate death may be a sudden accident or indeed be a gradually evolving disease. The end result is the same and both are of equal
Managing Risk and Resilience in the Supply Chain

care to the most senior management, its risk advisers and of course its stakeholders. A gradually developing disease, for example, a supplier’s quality problems beginning to affect the brand value, is no less destructive and can be more difficult to manage than a sudden loss. It raises difficult questions of reaction timing, not least the judgement between a hope that the problems can be resolved and a decision that the plug be pulled immediately and the disaster reaction plan, with its own costs and challenges, be triggered.

Within earlier business models, the organization managed most, if not all, aspects of its supply chain from within its own factory, office, warehouse and workforce. It had more than one way of interfacing with its consumers, and maintained stocks of finished goods and raw materials on site to keep it going for days or weeks in the event of a failure or slow down in supply. It employed the workforce directly and thus had day-by-day control over each one of the activities that were part of the final delivery of its product or service. It could also instantly redirect that workforce to meet any new urgencies that had emerged suddenly through an unexpected incident or need.

The model enables inventories (with their expensive capital) management as security demand to be kept to an absolute minimum, often just enough for a few hours’ productivity. It also enables the production levels and timing to match precisely with known demand or even pre-booked orders. It therefore dramatically reduces the dependency on accurate statistical forecasting of future demands that can only be based on past experiences and is always subject to variances and external risk influences. In this way, therefore, it can be used as a risk management value, not a risk management threat.

The modern business model, with its just-in-time supply chain, tight compression of margins, direct communication via the web simultaneously to millions of customers at home and abroad, is, however, much more brittle and has never been more susceptible to one single point of catastrophic failure. Furthermore, much of its workforce is now employed by a third party to deliver both intellect and activity, and only and precisely as agreed in a contract that had been negotiated at a time when the incident may not have been anticipated.

Outsourcing is no longer bolt-on for business, but an everyday way of life, at the local, regional, national and global levels. It is a way for businesses to focus on their core strengths and utilize the expertise of others to carry out the functions that the business is not as well equipped to perform. It is well named as a value chain: a name that illustrates that anything that happens in the chain of activities, from raw ingredient to final customer delivery, is designed to add value to that final product or service. If anything does not
add value or enables further value to be added, the activity is simply a cost drain and will surely be removed sooner or later.

Customers can move away so much faster – perhaps with just a click of the mouse – as indeed can competitors, upscaling quickly to steal customers. No longer do aggressive competitors, with the same business models available to them, need to raise capital, design and construct factories or office blocks and then recruit staff before they can upscale and attack a weakened organization. They simply sign a few new outsourcing contracts, maybe even with the damaged organization’s erstwhile suppliers.

Vodafone reports that it does not actually manufacture anything. In 2006/07, it spent more than £20 billion on purchasing products and services from third-party manufacturers which themselves source components and assembled products from other suppliers.

These models enable the organization itself to upscale and downsize much easier and more quickly than before and thus offers opportunities to spread risk and manage a crisis. A diverse supply chain can therefore be a useful risk-spreading tool as well as, when not effectively risk managed, a way of concentrating risk into single, potentially catastrophic, failure points.

The increasing importance of this wider potential for damage now lies at the very core of business models. It takes the risk manager and the most senior strategic managers of the organization way beyond the range of their financial risk management comfort zones, where, over many years, they have developed sophisticated financial risk models. It takes them into the much more amorphous and difficult arena of operational risk, particularly into areas of very low-frequency but very high-impact risks. It needs them to understand and respond to the fact that they are simultaneously shedding the ability to micro-control, shedding the very tools that they need, whilst exposing themselves to second-hand risks, impacts and frequencies much more difficult to evaluate, communicate and manage.

Throughout this book, the expression ‘risk manager’ does not just extend to those professionals who may carry this title. Generally speaking it will apply to those persons who have the responsibility to accept risk and/or give advice to senior managers that will place them in a position where they can make more informed, and therefore better, decisions about risk, impact, risk tolerances and risk management. This risk viewpoint can be from any director or manager who needs to address risks, and may come from a wide range of quite different risk-related titles across the organization.
Risk management has moved on from being simply the purchase of insurance products. Business continuity management is emerging from its own historical silo of technology and workstation replacement. Regulators are increasingly pulling operational risk concerns into compliance management, and even credit risk management should not fail to consider operational risks that could take away a debtor's ability to pay, nor indeed the single points of infrastructure failure that could affect separate debtors simultaneously. The realities of modern business models and their risks therefore cut right across these and the other silos of risk management that were, on the whole, previously able to deliver their values in isolation.

Risk exposures now have common roots and causes right across the whole spectrum of risk and strategic management frameworks. Of course risk management is as always as much about risk taking, and thus about opportunity, as it is about damage. Effective management of today's organizations therefore is not just about taking time out occasionally to consider risks, nor to search out ways that they can tick regulators' boxes. It is, quite simply, about good management, and, increasingly, survival. It enables the investment in activities and resources to be measured properly, and not only by the management itself but also by the organization's own stakeholders. Clearly a high return on a risky investment is just not the same value as a high return on a less risky one, a fundamental principle of business from time immemorial. The investor clearly wants a higher return if a higher risk is being carried, and above all, the investors of money, time, resources or reputation, need to be able to understand and measure the risks they are carrying.

Risk management is no less an enabler, when otherwise profitable opportunities are avoided because of an anecdotal fear of the risks that they may carry.

The outsourced value chain is clearly at the very heart of the resilience of modern day organizations, whether they are profit-making, public service or indeed charity. It brings real challenges in gaining an understanding of what those risks are, and indeed it brings a whole new range of risks and potential impact. The outsourced value chain also reduces or removes the manager's ability to micro-manage. It cannot hand over the responsibility for risk to third parties, but conversely it must delegate the management of some important risks to people whose relationship is only as defined within a precisely worded legal document.

These people must always put the interests of their own organization first as they are charged to do so by their own employers and stakeholders. The risks placed in their hands can be potentially lethal and include, not
least, the day-to-day ownership and management of crucial dependencies such as intellectual assets, the ability to deliver, legality, reputation, quality, compliance, the availability of workforces and their skills and experience.

This book sees the ‘supplier’ as a potentially crucial and urgent dependency. It sees the receiver as a dependency too of the ‘supplier’, which can be damaged or destroyed by the failure of the recipient’s ability to receive the goods or services as contracted, or to retain the supplier’s confidence that they are going to get paid for them. It sees the organizations further up the value chain delivering the organization’s products and services equally as ‘suppliers’ of these distribution services to the organization. The book sets out to explore the ways that supply chains can go wrong, either suddenly or gradually, and to discuss the strategic risk understanding and management of supply chains that are at the very heart of the effectiveness of modern day management.

This book therefore will explore these business models and in particular the dependency management that has become such a crucial management need, embracing not only infrastructures but also the other equally important corporate life support systems that we have listed.

Above all the book recognizes that outsourcing is so much more than subcontracting an individual task or the manufacture of items for the production line. It is about the strategic positioning of core elements of the organization and its dependencies into the hands of third parties.

Some outsourcing contracts are huge: in 2005 there were 11 deals valued at over US$1 billion. In a FM Global survey in 2006, ‘supply chain’ topped the list of risks causing major disruption. A survey by AON lists ‘loss of reputation’ and ‘business interruption’ as key concerns, both of which are supply chain dependencies. An interesting case study to set the scene is The Association of Clearing Houses.

The Association has three main constituent companies: Cheque and Credit Clearing Company Limited (bulk paper clearances); CHAPS Clearing Company Limited (same day electronic clearing); and BACS Ltd (bulk electronic clearing).

CHAPS provides core services to 29 banks and financial institutions clearing on average £200 billion a day. This is just part of the picture. BACS, the automated clearing house, handles 14 million electronic debits and credits a day, averaging £9 billion. A high peak day would see 57 million transactions and 80 per cent of UK adults are paid through the BACS system. In addition, the company handles cheque and credit clearing, debit and credit card transactions and processing, and ATM and cash transactions.
Moves to real time settlement have increased single points of risk to exposure that would simultaneously damage or delay these millions of financial transactions and perhaps even the country’s economy. Just one of the lessons addressed after the September 2001 debrief was that, whilst there is diversity of backup data, there may not always be diversity of control systems and indeed it is likely that some routings previously perceived to be diverse, actually converge.

The widespread and simultaneous impact of damage by such a service supplier organization could destroy its customers’ own continuity plans. Whilst risk activity can be delegated, the responsibility for risk cannot. Dependence on such organizations therefore demands that the recipient organization itself ensures that those exposures are controlled and can illustrate that risk control to its customers and regulators.

In summary, the responsibilities and demands of the strategic management of an organization do not change when a part of the core activity is repositioned with a third party. Understanding and retaining control over the risks of those activities, and retaining at the same time the freedom to fully exploit their commercial value, does however bring very different problems, balancing acts and challenges.

David Kaye  
FCII FBCI FRSA MIRM  
Davidjkaye@aol.com
Risk management and modern day business models

Impact vs risk

A risk manager will routinely consider not only the risk of something happening that could divert the organization from its objectives and responsibilities, but also the likelihood and/or possible frequency of such an incident. Equally important to the risk manager is precisely how the likely impact of that incident could damage the individual sensitivities of the organization and its people. Understanding that impact entails a strategic understanding of the commercial activities of an organization, its role within its market-place, its differentiated positioning from whatever competitors it has, and its sensitivities to holding that positioning.

It also entails understanding what makes the organization tick and the wide range of hard and intellectual dependencies that are keeping that organization in its position. Each organization will have its own individual sensitivities, just two of which will be the ability to remain legal, and to continue to deliver to its own range of stakeholders all of the expectations that have emerged ‘in the good times’.

As part of the risk policy statement, the risk manager will have defined graded levels of impact for ‘risk-taking colleagues’, i.e. all those responsible for a division or support function. This will not only include financial cost; indeed one challenge is to grade financial and non-financial risk in a consistent way. It will include the impact of the organization’s inability to deliver on its promises to stakeholders and becoming weaker within its market-place. This will naturally embrace those things that are crucial to that ability to deliver as promised. As a consequence, the element of ‘maximum possible time out’ is one of the crucial assessment criteria and this will vary from organization to organization and by type of business.
Managing Risk and Resilience in the Supply Chain

The risk manager will base advice to the board or chief executive on these dimensions of risk and impact who will need to decide whether the organization has the strength and resources to accept such risk and/or impact, or whether one or more of the risk, likelihood or impact needs to be managed down to acceptable levels.

Once the risks are identified and evaluated, the risk management toolbox, in headline form, embraces the options of:

- accept the risk and impact;
- reduce the risk down to tolerable levels;
- reduce the potential impact down to tolerable levels;
- transfer the risk to a third party;
- prepare financial plans to enable the monetary cost to be funded;
- prepare carefully so that the strengths and resources of the organization can be used to manage an incident through and thus contain the impact within acceptable levels.

The organization may decide that the worst-case scenario is one that it could manage through without unacceptable damage. It may decide to remove itself from an activity or responsibility because the risks from that activity are unacceptable, or the cost of risk managing them is too high. It may alternatively look at the potential impact on it of a risk incident and then take steps to control that impact. An obvious example is to back up electronic data frequently and store that backup data well away from the primary risk site.

It could transfer the risk to a third party, say by contract with a supplier, customer or other counterparty, or transfer financial risk by way of insurance. (We will explore residual risks in doing so later in the book.) The organization may decide that the most effective option is to use the strengths and skills available to it by preparing and pre-resourcing business continuity plans.

We will explore these headlines in more detail as the book unfolds. At this time it is sufficient to say that these tools are not exclusive and the advice is likely to be to use a combination that best and most economically meets the risk challenge.

We will also explore and develop the point that risk management is not just an operational management issue. It is equally a strategic management issue and begins at the very first stage of ‘should we outsource and, if so, for what reasons and objectives?’ We will explore the concept of the cost–benefit analysis that does not only measure immediate financial cost and gain, but
which also measures risk. This book’s definition of ‘cost and benefit’ includes the more indistinct, but crucially important, costs and benefits of quality controls, reliability, reputation, management information, flexibility, and both the value and cost of risks being carried.

**Hollow organizations**

What are now described as modern day outsourced business models have not in any way changed the objectives or the responsibilities of any organization. Rather, it is just the way that they work towards those objectives and how they deliver their products and responsibilities that has changed. Organizations are taking the opportunities of instantaneous database mining, international communications bandwidth, macro and micro technological delivery and communication tools and also the removal of trade barriers that have opened up opportunities to cross physical and political boundaries with ease. With a global, rather than national market-place, this has enabled the true global organization that can sell and deliver worldwide and also resource its value chain from that same worldwide playing field.

One by-product has been the sheer scale of these organizations, which, through inherent growth, mergers, acquisitions and multinationalism, now stride the globe with relative ease. Another by-product of the ability to micro-mine huge databases is the ability to communicate with each client individually and also differentiate the product, customer by each individual customer.

As has been said, outsourcing is so much more than subcontracting, and certainly has moved on significantly from just a way to reduce costs.

---

**BMW manufactures the Mini in the UK, using parts supplied from, and selling this product around, the world. The production line process is computer driven and enables the customer to decide on the individual car from a choice of 250 detail ‘packages’ of engines, models, trim, wheels and other accessories and parts.

The ingredients of that individual motor car – matched at the beginning of the production line to its own customer – are fed right throughout the supply chain and then, at the precise moment and sequence, into the final production line.

Another opportunity for some businesses puts information, rather than bespoke machinery or a particular workforce, at the very heart of customer
Managing Risk and Resilience in the Supply Chain

delivery and indeed now as its driver. Information, especially electronically stored and accessed information, is of course much more portable than either machinery or people and, as long as it meets local laws, can travel and be accessed around the world instantly and without any constraint.

WS Atkins and other similar organizations provide call centre services to a wide variety of very different clients and types of business. The same WS Atkins call centre operative can, during the working day, provide a customer telephone response to a whole range of industries and organizations.

The telephone number that the caller has used tells the software which organization that customer expects to contact. The software and database then provide the call centre operative with the answers to most questions without the need to be experienced in the intricacies of the individual client organization’s business. Electronic communications then immediately set in motion the actual services agreed: either directly with the principal or, again, by instructing another outsourced service supplier.

These and similar call centre services suppliers are of course in the front line of sales and other customer relationships and can, with the increasing bandwidth of international communications, be in any country in the world, not only the currently popular countries of Ireland, India and the Philippines.

Another value of the flexibility possible by outsourcing to a third-party specialist is the ability to turn the old business model on its head in another way. The old model means that the manufacturer or service deliverer produces the product and then sets out to find a customer for it – a supply-led value model. The flexibility and speed now possible enables the product to be sold and then created – a demand-led value model and one that transforms the stock risks and cost implications.

The ultimate outsourcing contract is to enable customers, via the internet, to gain direct access to the software and databases and to then deliver the organization’s service promises to themselves. This is now common in many industries, not least the financial services industry and in airline, theatre and hotel bookings.

This means that all of these opportunities move to the heart of the organization’s existence and thus become massive dependencies too. As said, this is the strategic positioning of entire sectors of the organization into third-party hands. The relationship makes them a partner and, even with effective risk management, makes each dependent on the other for the survival of that partnership and the ability of these new strategic business shapes to survive.
‘There are many innovations in the new Boeing 787 but perhaps one of the most innovative aspects could be the way in which it is being built. For previous models, Boeing played the traditional role of main manufacturer, contracting with an army of suppliers for individual parts and systems, and then laboriously assembling them into the finished product. This time around, major suppliers will design and build entire sections of the plane, shipping them to Boeing for final assembly and testing at Everett, WA. Various components might travel around the world, passing through multiple contractors, before ending up at their final destination. In this way, the majority of each aircraft will actually be built by Boeing’s global partners.

The plan will lessen the need for Boeing’s own resources while speeding up construction. Each aircraft will be assembled over a three-day period. To make that possible, Boeing had to achieve a whole new level of collaboration with key suppliers around the world.

“Instead of multi-tiered suppliers, we truly have partners,” says Tim Opitz, Director of production and support systems for Boeing Commercial Aeroplanes. In all, the company is relying on 135 locations around the world for manufacturing and fabrication. With responsibilities spread so thinly, the slightest delay at any point in the supply chain could paralyse production.’

(Robert Bowman, Global Logistics & Supply Chain Strategies, 1 March 2007)

Many a 21st century organization can now therefore be described as a ‘hollow company’: a corporate life form that consists only of its entrepreneurialism, stakeholders, a small control team, legality, brands and other intellectual assets. The entire supply chain and delivery chain is then supplied by third parties under contract.

There is a risk implication also that the modern, outsourced business model is much leaner and with much less margin for error. Its ability to absorb surprises is much reduced; the potentially catastrophic risks are more focused into one single failure point, and thus the understanding of its risks and managing them has never been more critical.

All this has dramatically shifted the dependencies and indeed the weak points of modern day organizations, but equally it has raised expectations way beyond previously recognizable levels. Customers now expect simultaneous access to their personal information, immediate answers to their questions and instantaneous delivery of the product or service required.

The modern data risk manager has these very few but each potentially catastrophic dependencies as the focus of risk understanding and risk management.
work. In these models, there are: new relationships, new dependencies and above all new expectations to manage.

As stated at the beginning of this book, an organization’s objectives and responsibilities in concept remain just the same but there is little common ground between the playing fields of the earlier generation of risk managers and those of today.

The stakeholder

No discussion on organizational risk is complete without looking at the organization’s responsibilities through the eyes of the various stakeholders. It is indeed the stakeholders of the organization who are the ‘customers’ of the risk management processes as it sets out to deliver on its promises and not expose the stakeholders’ interest unduly to unexpected loss.

Even if we can now summarize an organization more simplistically, the list of stakeholders remains almost unaffected. Also, the underlying responsibilities of the organization to those stakeholders remain just the same.

We can usefully split the stakeholders into two categories: those who are stakeholders throughout the good times and those who become stakeholders when they react to an organization in distress. Some stakeholders cross this boundary of course but it is useful to keep this split in mind, even if only to ensure that we do not forget the latter category in our risk and response management.

We will also need to remember that individual stakeholder expectations and demands can be in conflict with each other, turning some decision making into a challenging balancing act. This is especially so whilst an organization is trying to manage a fast-changing, potentially disastrous incident with reduced people, resources and communications, and in the media spotlight.

Types of stakeholder

Stakeholders can be divided into two main categories: those who are continuing stakeholders during the ‘good times’, and those who become stakeholders by their reaction to an incident (the ‘bad times’) and, in so doing, can also be
Risk management and modern day business models
categorized by their ability to influence the outcomes of that incident (see Table 1.1).

<table>
<thead>
<tr>
<th><strong>Table 1.1 Stakeholder categories</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>In good times</strong></td>
</tr>
<tr>
<td>Employees</td>
</tr>
<tr>
<td>Customers</td>
</tr>
<tr>
<td>Distribution channels and intermediaries</td>
</tr>
<tr>
<td>Suppliers</td>
</tr>
<tr>
<td>The stock market</td>
</tr>
<tr>
<td>Other financiers</td>
</tr>
<tr>
<td>Partners</td>
</tr>
<tr>
<td>Trade and trading standards</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

‘Good times’ stakeholders

Employees

Most employees need a job to sustain personal and family life and also self-esteem. The organization’s responsibility to employees is of course to continue to provide them with gainful employment.

The relationship however goes beyond this. To gain the best out of an employee workforce, the employer needs to ensure that the workplace is as safe as is reasonably practical. This is also essential to maintain the workforce’s morale, trust and pride in the organization for whom it is working.

Those employees who have invested their careers, lifestyles, time and self-esteem in the particular employer have unarguably become stakeholders, and
will remain as long as they still have trust and pride in the organization. Their response to an incident can become second category ‘bad time’ stakeholders too. If the employer cannot maintain their trust as they struggle to handle a risk incident, then employees will worsen the situation significantly by walking away. It is always the best employees who will move on the quickest, by the fact that they are the ones with the greatest choices, and certainly headhunters will target an organization in distress and only be interested in the better employees.

This makes communication and employee relationships very important priorities in business recovery management, not least when the employer, facing unusual and stressful circumstances, needs employees to work beyond the employment contract to keep the organization alive.

Outsourced employees will always of course remain subject to their own employer’s directions and priorities. Any workforce flexibility can only be expected within the framework that was set in the detail of the contracts drawn up in the ‘good times’ with their own employer, the outsourcing company. One of the first risks and impacts therefore of an outsourcing model is the loss of the ability to micro-manage the ‘workforce’ at all times. This is a subject for a separate section later in the book.

Customers

Customers will remain only whilst the organization can continue to deliver the contracted services or products on time and to the expected quality. An unexpected and unmanaged risk incident can damage this ability. There is, though, more than that. Customers will remain as long as the expectation is that they can continue to receive the expected services or products on time and to the expected quality. Customers therefore can be lost long before there is an actual reduction in service levels and once again this makes customer confidence a power to be actively managed in the ‘bad times’.

If a customer loses confidence, perhaps by hearing of a risk incident in the organization, the customer (equally whether an end consumer or another business in a value chain) has almost always the choice of moving away to a competitor. Often the debate – once confidence is lost – is only around just how quickly, legally and operationally that change can be made. With modern distribution channels such as e-commerce, customers can move away much quicker than before. Indeed, entire distribution channels can move away in seconds by the touch of a keyboard mouse.
In 2007, Northern Rock found itself in a position where it needed to go to the Bank of England for what are sometimes known as ‘emergency funds’. This was caused by inter bank loans and financing drying up quite suddenly due to money market concerns about where precisely the final damage emerging from sub-prime loans was located. This request for support became known and depositors became concerned about the safety of their own deposits with Northern Rock. This concern heightened dramatically when the website capacity became overpowered by unplanned for levels of simultaneous enquiry. Customers could not gain routine access to their accounts and information and therefore became even more concerned.

They then did the only thing still available to them and that was to go to a Northern Rock branch to withdraw their money – a classic ‘run on the bank’. Branches could not cope with the levels of simultaneous demand and long queues formed. These long queues caught the attention of the media – pictures and film were broadcast widely raising the temperature of these and other depositors even more.

This increased Northern Rock’s existing liquidity problems dramatically with massive additional reputational risks and cash flow damage.

Even public service organizations and monopolies need to retain customer confidence as part of risk management work. In the event of a failure in trust, or a risk incident that removes the ability to gain access by normal channels, customers will feel the need to search for reassurances or take steps to manage that feared impact by themselves. That search may be wholesale, exceeding normal workflow expectations and affecting parts of the organization that are not resourced to cope with such a large flow of enquiries.

This can cause an impossible strain on resources, bringing an already struggling organization to the point of total collapse.

Special cases

Some business models depend entirely on a relationship between supplier and customer remaining orderly and confident. A bank and an insurer need above all to be trusted and they assume responsibilities by contracts that involve billions of pounds. To enable them to gain value out of those premium and investment deposits, they place them in investments that are longer in term than the contracts with their own customers. This assumes that the demand for the return of these funds follows predicted patterns. A run on a bank, as
in the Northern Rock example, due to loss of confidence could mean that they need to realize assets quickly from a long-term investment portfolio. Very large volumes of shares placed together onto a stock market can, in themselves, cause a change in the demand and supply balance and cause the price of those shares to fall. Again, existing problems are greatly exacerbated.

There may be special requirements in some contracts that are a core need. Contracts to supply the military or police, for example, will have special demands on information security. Even a small risk incident, if it destroys such special needs, can bring the whole contract to a close.

The impact, urgencies and sensitivities when supplying another organization within a value chain are of course much higher than those of individual customers. A failure to deliver can have an immediate impact on the others’ own time-critical processes. Consequentially, a failure to deliver a tiny, and perhaps thought to be inconsequential, ingredient, can have massive impact further up the supply line.

It is likely that the receiving organization has contingency plans in place in case of such failure. It is likely to have other contingency suppliers ready to step in immediately, thus instantly taking the damaged supplier organization out of that chain, probably permanently. This could turn a temporary failure into a total disaster for the supplying organization. This is especially damaging where the supplier contract is such a significant part of the organization’s revenue that its loss destroys its own economic viability. One example could be where the produce a farmer supplies to a supermarket is such a large proportion of the supplier’s business that, in the event that the one contract is lost, the business cannot then meet its other fixed charges and costs.

We will frequently stress that the risks around supplier/customer relationship dependencies are two-way. There is a mutual dependency and, either way, that dependency can be organization critical.

In 2007, Gloucestershire in the UK took its turn to have devastating floods affecting tens of thousands of homes, infrastructure services and businesses. Farmers’ produce was widely ruined but they found themselves in fixed-price contracts with supermarkets with no relevant escape clause.

Even though a normal demand/supply equation would enable prices to rise (and thus enable farmers to cover costs and survive on less output), the contracts meant that they could only charge the prices that had already been contracted into the relationship prior to the floods.)
Risk management and modern day business models

Just like employee relationship management, confidence in the ability to supply into the future is a crucial ingredient of just-in-time logistics management. The receiving organization can – and will – move away quickly and totally should that confidence alone be damaged by a risk-based incident. Any financial or other penalties, and the brand-damaging publicity associated with them, that are built into the wording of a contract, can be devastating to an organization that is already reeling from an unexpected operational incident; yet the risk incident may only have damaged confidences.

Distributors

The responsibilities to distributors are indistinguishable from those to individual customers, except by the volumes involved and perhaps by contract wording that will set in law the ownerships and responsibilities at each step of that relationship.

This is no less so when the recipient of the goods or services ‘white labels’ them by building them into its own brand name and marketing.

Where the customer ‘white labels’ the product, i.e. sells it on under its own brand name and packaging, there may be a different reputational issue to be managed than when the product retains the supplier’s own name and packaging.

A drug store chain such as Superdrug or a supermarket such as Tesco may choose to retail something under its own brand name – this could be anything from shampoo to breakfast cereal. This is a commercial balancing act between wholesale/retail critical mass, packaging costs and any necessary investment in awareness of the lesser known of the two brand names.

Where the ‘customer’ chooses to ‘white label’ the product with its own name then it carries additionally the brand and reputation risks of failure, quality problems and even, if necessary, product recall.

Suppliers

The challenges with suppliers, the primary subject of this book, are two fold. The business models discussed mean that organizations, however large, find themselves totally dependent on the timely delivery of another organization’s ingredient, service or intellectual asset. Sometimes ‘timely’ is measured in
hours rather than days, or even, in some e-commerce models, simultaneous with the need.

Loss of life and injury apart, many of the greatest problems facing large organizations after the 11 September 2001 terrorist attack was that, whilst they themselves had a global reach and alternatives, they found that they depended on small but critical suppliers who, without the alternative resources of a multinational, were destroyed.

One example was a small software house in the same building that had been contracted to design, deliver and maintain software that was integral to the large organization’s own delivery chain. The failure of that software house in the terrorist attack meant that the large organization did not have the software codes that would enable other technicians to continue to maintain the software.

The second supplier-based challenge could be that the supplier, hearing that the customer is weakened by a risk incident, may need reassurances about its continuing ability to pay. It may be difficult to give reassurances that are satisfactory to that supplier. There may then be a demand to pay before the service is received, which creates new cash flow challenges that can in themselves be difficult to satisfy. The perceived higher credit risk of the now damaged customer could create a demand for more expensive or shorter credit terms that, in themselves, could undermine the organization’s financial models and pricing.

The stock market

It can be said that the stock market operates to its own valuation rules, often with little bearing on the underlying value of the organization. Whilst it has indeed a range of influences such as political risk, the competition for capital, and takeover activity, this would be a dangerous simplification.

Public investors and their advisers, stock analysts and credit agencies look not so much at whether the company is making profits, but whether it is about to declare values and dividends in keeping with current expectations. The market does not like surprises at all and will downgrade a share if there are reasons to be concerned that it may be unable to meet its earlier promises. ‘Profit warning’ statements to the market that downgrade current expectations are very likely to cause a fall in stock value, whether that is as a result of a
trading downturn or equally following a risk incident that has removed the company’s ability to deliver as promised at the year end.

There are statutory and market regulations that demand that quoted companies keep the market advised of risks being carried and we will discuss these later in the book. Furthermore, a significant reduction in stock value will reduce the relationship between that value and the amount of current borrowing, i.e. the company’s ‘gearing’. The higher the gearing, the greater the perception of less strength, thus the company’s cost of current and further capital borrowing may increase. Organizations equally need positive cash flows as well as capital and revenues. This may turn a short-term crisis into a long-term cost of finance problem that may destroy the financial models on which the company is founded.

Other financiers

Whilst possibly less regulated, the principles above apply equally to other financiers of an organization. It could be a government that is financing a project or non-governmental organization, a charity raising funds from donations or indeed a subsidiary looking to its parent to finance development.

Private financiers and partners too will be looking for confirmation that the organization is setting out to understand its risks, communicating them and managing them effectively. They may stop future funding or even be able, under the contracted relationship, to demand the return of funds already supplied.

Partners

‘Partners’ may come in all shapes and sizes, from individuals to large organizations. The relationship may be informal, defined by contract or be a significant shareholding and working relationship in a quoted or other legal entity.

Partners invest more than time and money. They invest their reputation – formal brand values and other confidences – and also the opportunity cost of choosing this particular activity over others. They are therefore important stakeholders, relying on each partner to manage the risks that could destroy the other.

The partnership agreement may well define legal liabilities and ownerships between partners but the rights in law defined by these agreements are of
value only when the organization or person being sued has the means to meet any agreed liability for their failure. If they are ‘of straw’ (or become ‘of straw’ because of the incident) the legal rights are worthless as they are uncollectable. They are most certainly no substitute for effective, two-way, risk and impact management.

Trade standards

A risk creating a damaging incident may have the effect of removing quality control and bringing the organization to the attention of its fellow market players and, more formally, trading standards regulators. The brand value is damaged, as is the wider confidence of current and prospective customers and other stakeholders.

*Stakeholders emerging in ‘bad times’*

Whilst some stakeholders can fit in both the categories described on page 6, the following stakeholders are usefully considered primarily for their ability, indeed propensity, to cause further damage just as the organization is already struggling to respond effectively to an unpleasant surprise.

The natural environment

Organizations are increasingly facing expectations that they respect the natural environment and the safety of the environment within which they operate. This not only means a demand that they do not actually harm that environment, but also, increasingly, they are expected to proactively protect or improve the environment around them.

They need to respect their neighbours’ access and ability to operate and thus not allow a risk incident to damage them too. They may find that their ability to respond to a damaging incident is constrained by these responsibilities.

They may even find that the public services are not able to assist as fully as expected. A fire and rescue service may, for example, not be able to pour water and chemicals on a fire if the run off from the building’s contents will contaminate the natural watercourses nearby. The fire and rescue service
and the organization’s own recovery teams may be held back from the site by police controllers who consider the site as yet unsafe for human entry, or indeed as a scene of crime.

Therefore, we have two challenges for the risk manager. One is to ensure that the organization will protect, i.e. risk manage, the ability to meet these responsibilities. The second is to understand the constraints that may dramatically increase the maximum probable loss of an incident.

Customers (again)

An occurrence of damage or potential damage to customers is not just about keeping them as customers thereafter. There may be indemnities to pay for damage caused and also, perhaps even more difficult, huge numbers of products may have to be recalled, should they be considered unsafe or not of ‘merchantable quality’.

The process of recalling products is a hugely difficult one, especially as it is always conducted in the eye of the public and the media. It is a greater challenge when the cause of the lack of safety lies deep in a supply chain and the distributions lie deep within a delivery chain. Those difficulties are operational, intellectual, legal and often technological, and are discussed later in this book.

The legal environment

It is an obvious point that the organization must always remain legal within each legal jurisdiction within which it operates. This embraces civil law, criminal law and the host of regulatory requirements that are demanded around its activities, people and products.

The risk manager needs therefore to be aware of these requirements and when developing the risk management envelope around the organization ensure that these needs are being met and will continue to be met, whatever happens.

Regulators not only expect organizations to be compliant but expect them to be able to demonstrate that they have been compliant and continue to be compliant. If the compliance audit trail therefore is not secured against any risk incident, that loss could be the very first cause of organizational death.
The power of a regulator is not just to impose financial penalties. The publicity can destroy brands and confidences, and the regulator can demand compensation be paid to third parties, alter credit ratings and, above all, instruct a cessation of trading.

The regulator may bring its own unique demands and requirements. During the UK financial services scandal of the 1990s when organizations were accused of misselling pension contracts, the Financial Services Authority demanded that the companies write to each of their pension fund customers. They were required, in effect, to ask customers to let them know whether they felt that they had products missold to them. They were then required to respond to each reply individually.

Professional indemnity insurers’ policy wording precluded the insured financial services companies from ‘soliciting claims’. Caught between them both, many pension fund providers had to take in a huge administration burden and reimburse customers without the benefit of professional indemnity insurance recoveries.

The media

We have already mentioned the importance of brand and reputation – one of the small number, but crucially important, headline dependencies of a modern organization.

The media is, of course, a wholesale purveyor of brand values and indeed, conversely, destroyers of brands and confidence.

An attack by the media, whether justifiable or not, can be destructive to the entire organization and its positioning. The attack may not be directed specifically at the risk manager’s organization but may be an attack on the work environment within which the organization operates or, relevant to this book, on one of the suppliers with whom the organization is identified.

Again, a strategic risk issue is to operate the business ethically and well so that it reduces the risk of attack. The media risk can be managed too by ensuring that media management resources and skills are ready in place for use during an attack or as a risk incident unfolds.

Doing nothing may not be an option. Any failure to communicate too often creates gaps that are soon filled with rumour, whispers, vested interests or just simply malice.
Potential customers

We are in this chapter considering the potential impact of stakeholders which become so by their reaction to a risk incident. We have already mentioned brand and confidence with regards to the media, above, and also with regard to existing customers and other stakeholders.

The risk management of an incident will also affect the confidence of the wider public and especially those who may become future customers. Reputational damage that destroys the sales team’s ability to produce new orders going forward can not only be damaging but can also be destructive.

Conversely, it is possible, by effective risk management and communications, to use a damage situation to good benefit by illustrating clearly how seriously the management takes its responsibilities, even during the diversion of unexpected damage.

Competitors

Competitors read newspapers too and a weakened competitor may be seen simply as a business opportunity. They can, using the macro- and micro-communication tools that are now available, set out to target customers with offers and marketing. The damaged organization may wish to secure as best it can its market position by fighting back with discounts and offers of its own. The cost of those offers are no less a cost of the incident itself.

With the opportunities of outsourcing and offshoring, these competitors do not need to raise capital, obtain planning permission, go out to tender and then build factories before they begin to compete. They do not even need to recruit and train a workforce. They simply need to set up a new range of outsourcing contracts, perhaps even with the erstwhile suppliers to the damaged competitor.

These are real impact assessment factors for risk managers and their boards and management to consider. Public service organizations and charities also have competitors for the purses that supply them. A public service organization losing the trust of its masters or stakeholders for any reason may cause a shift in responsibility to another department or even an approach by a private finance initiative.
Potential competitors

The removal or weakening of one player in the market-place may reduce competition to the point that a third party sees the new demand/supply imbalance as a worthwhile opportunity emerging for it in that particular market-place.

The opportunities now to enter a new market without huge initial investment are the same ones, and just as quick and easy as an existing competitor setting out to upsize.

Third parties

An organization and its people remain subject to the civil law of their playing fields and if they harm other people with their activities or products then they must expect those people to litigate against them.

The level of damages awarded may far exceed the free assets of the organization, especially in some jurisdictions, such as the USA and Canada, where the awards may include huge punitive damages as well as indemnities. These and other jurisdictions may demand that one defendant is jointly and severally liable for the whole claim, even if it only contributed to the cause of the loss.

Most, but by no means all, such liabilities are insurable and arranging insurance and indemnity levels across a diverse organization and against incidents that can only be guessed at is one of risk management’s minefields. We will explore this in more detail in a later chapter.
Bringing stakeholders and risks together

We have now begun to look at some of the potential ways that a risk incident can damage an organization and its wide array of different stakeholders. We can now begin to build a matrix of these responsibilities against the operational dependencies that, if lost or damaged, can cause unacceptable damage to them.

Before we do so, there is value here in a reminder that all activity is risky to a greater or lesser extent. All commercial activity is a fine balancing act between risk and reward and the risk manager’s responsibility is not to remove all risk. Rather, it is to ensure that boards and managers make better-informed, and thus better-quality, decisions around this balancing act of risk and reward. We will proceed therefore to deal with risks where the full and wide-ranging consequences have been evaluated and found unacceptable.

We also need to make another assumption, and that is that the risk levels thought acceptable to the management have been communicated clearly to the stakeholders and have been accepted by them too.

<table>
<thead>
<tr>
<th>The board of a multinational insurance company accepted that its balance sheet, cash flow and revenue strengths allowed a risk tolerance level of £1 million per incident. The board agreed to accept that potential loss for its net account and reduced its insurance covers accordingly, saving a substantial amount of insurance premiums.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Its subsidiary in South Africa had a minority local shareholder and operational partner owning 40 per cent of the shares in that subsidiary. That decision in effect imposed on that shareholder a potential unprotected loss of £400,000, a level well beyond that shareholder's tolerance levels.</td>
</tr>
<tr>
<td>Clearly, there is a massive responsibility to advise that shareholder and perhaps join in arranging internal insurance or other protections.</td>
</tr>
</tbody>
</table>

Stakeholders: a summary

The management of an organization has many different stakeholders to which it has quite different and sometimes conflicting responsibilities. Furthermore, suppliers’ own reactions to risk can in themselves create or add to potentially
disastrous scenarios that need to be anticipated, protected against and perhaps even managed through as they happen.

The supply chain participants, as stakeholders in the organization too, fit into the organization’s risk profiles both as a dependency and a responsibility. The damage that can emerge from supply chain participants is potentially catastrophic and as soon as any one of them in the (sometimes long) chain fails, the organization next in line is affected. A supplier that perceives weaknesses in its customer, the next receiver organization in the line, may withhold supply. That change leads to far-reaching damage to many relationships. A different cause of loss, perhaps, but, sadly, the same damage to the final customer delivery.

This is not the most comfortable of messages when the decision to outsource has removed core elements of resources, information, customer relationships, workforce control, legality, brand and other dependencies out to that third-party organization. Getting them back again has many operational, legal and practical problems to overcome that can remove the organization from its fast-moving market-place.

Back to basics

The risk manager can be involved at all levels of risk within the organization. The total monetary cost of low-level, high-frequency losses within one accounting period can be risk managed out by effective investment in risk measures. An example would be the shoplifting risk across a chain of supermarkets. Risk measure investment could see increased security around warehouses, redesign of the shop floor, increased CCTV and other security, increased vigilance at staff exits and more security floor walkers around the stores and at exits. Additional measures include supporting the local police and using radio/telephone warning systems between retailers when known shoplifters are recognized.

These risk management activities have relatively routine cost–benefit balancing acts to evaluate and implement. The subject here, however, is the resilience of the supply chain, so we will go on mainly to discuss the more difficult risk challenges of managing potential loss or damage that can threaten the very viability of the business model, and indeed the very survival of the organization. The just-in-time, business-critical supply chain dependencies
Risk management and modern day business models

bring these kinds of challenge. These exposures are critical to the crucial dependencies that have already been defined as:

- enabling continuing entrepreneurialism;
- a wide range of stakeholders;
- the small control team;
- legality and compliance;
- brands and wider confidence;
- other intellectual assets; and
- the (mostly outsourced) supply chain and delivery chain.

This book will stay with supply chain risks but must, to be meaningful, embrace these other exposures insofar as the supply chain brings risks to these dependencies.