Today, local authorities are in the midst of a significant period of change and have a new role and purpose as community leaders. This includes dramatically increasing the level of outsourcing and working with partnerships to deliver on promised outcomes. Indeed, Government policy has moved from encouraging partnerships towards mandating them.

We have, sadly, a very wide range indeed of disasters and embarrassments caused by supplier and partner failure that encourages us to place these risks as topical, potentially catastrophic and urgent. These third parties are very likely to have different agendas, ambitions, stakeholder pressures to satisfy, governance standards, attitudes to risk acceptance, levels of resources to apply to risk management, sensitivities, and often very different business and human resource management cultures. Once these relationships are created, stepping back from them is not easy, especially urgently and when in a crisis.

This Briefing Paper makes the fundamental point that outsourcing or partnering, whether it is towards back office or front office outcomes, is so much more than subcontracting or logistics management. Never before has outsourcing and its risks, myths and opportunities been such a topical and urgent challenge for public service executive leadership and its managers. This Briefing Paper sets out to support them in understanding and addressing these issues.

David Kaye

David Kaye is a leading author, lecturer, examiner and workshop leader on risk management and business continuity subjects. He guides a diverse range of companies and public sector organisations on risk related issues around the world.

David started his working life at Eagle Star insurance, becoming CEO of subsidiary insurance companies within the group, living and working in five different countries.

David’s latest book, Managing Risk and Resilience in the Supply Chain, published by the British Standards Institution in 2008, is a core textbook for universities and business schools. He is the Institute of Risk Management’s lead examiner in business continuity and is the author of Chartered Insurance Institute’s textbook on operational risk and a standard book on business continuity. David is a Fellow of the Chartered Insurance Institute, a Fellow of the Royal Society of Arts, a Fellow of the Business Continuity Institute, and a Member of the Institute of Risk Management.
## Key risks – expert vs public assessments

<table>
<thead>
<tr>
<th>Expert ranking</th>
<th>Risk</th>
<th>Public ranking</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Managing partnerships with other organisations</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>Funding and good financial management</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>Human resource issues</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>Crisis planning</td>
<td>8</td>
</tr>
</tbody>
</table>
1.2 Outsourcing and partnership working

This paper makes the point that outsourcing the supply chain and partnership working is so much more than simply subcontracting or logistics management. Outsourcing places what have been entire and core elements of the home organisation, into the hands of third parties. The core elements that are passed over are not only workforces and their skills, it is also the physical resources that are needed to deliver on the promises. This raises a wide range of control and quality issues, but also, other equally vital foundation stones are passed over. These include:

- a very wide range of intellectual assets
- the ability to remain in control
- risk management processes and attitudes
- legality
- compliance
- information and other security
- the ability to communicate with stakeholders
- and also the vital need to ensure continuing confidence in the Authority itself

Local authorities are now increasingly entering into a broad range of relationships across the public, private and third sectors. Nothing is ruled in – and nothing is ruled out. Many of these relationships underpin the operations and service delivery of the entire local authority, whilst others are outsourcing partnerships focused on achieving the target outcomes laid out in the Local Area Agreement (LAA) and the Local Strategic Partnership (LSP) – and measured by the Comprehensive Area Assessment (CAA).

The Audit Commission refers to organisations working together to achieve an outcome as a “delivery chain.”

Yet a closer examination of the broad range of relationships that a local authority engages in across the public, private and voluntary sectors reveals an even more complex story. Indeed local authorities are establishing different types of supply chains – each with their own attendant risks and challenges.

These third parties are very likely to have different agendas, ambitions, stakeholder pressures to satisfy, governance standards, attitudes to risk acceptance, varying levels of resources to apply to risk management, sensitivities, and often very different business and human resource management cultures.

Once these relationships are created, stepping back from them is not easy, especially urgently and when in a crisis. Reinstating the home organisation’s ability to deliver, and to regain control of vital dependencies, may need them to overcome operational, human, technical, legal and practical problems that, if achievable at all, will in the meantime stop delivery of crucial and urgent services.

In the context of this guide, supply chain management is concerned with the “co-ordination of all parties involved in delivering the combination of inputs, outputs or outcomes that will meet a specified public sector requirement.”

1.3 The responsibility

The day to day function of risk management realistically must often be delegated but responsibility for failure cannot be so delegated. All risk-measured management therefore needs to include governance and control procedures to ensure that the organisation does not stray unknowingly beyond agreed risk tolerances; now or at any time in the future. Imposing this control environment is the first responsibility of a chief executive; without this the job is unachievable.

In an outsourced delivery model, the chief executive’s and the authority’s responsibility is not at all diminished. It is however more focused and can effectively be summarised as:

- The effective and risk-aware creation of the relationship
- The retention of statutory responsibilities and in tort
- Ensuring effective monitoring, risk information and audit

- Constantly retaining the ability to be flexible and to manage change
- Ensuring that there is the ability to exit as necessary without failure of responsibilities and in critical service deliveries

This paper acknowledges and works within government guidelines and requirements, not least Audit Commission requirements and, again, such drivers for outcomes such as the Comprehensive Area Assessment. These include the Key Lines of Enquiry (KLOE) document:

KLOE: 2.4 Does the organisation manage its risks and maintain a sound system of internal control?

This individual KLOE has a focus statement that requires that ‘the organisation has effective risk management which covers partnership working.’

1.4 The nine myths and minefields within outsourced delivery

It is unarguable that the delivery of crucial services through a range of third party organisations means that the risks being carried are more opaque than when the delivery is all in-house. To support the understanding of these challenges this paper identifies and explores some commonly held myths about risk, the responsibility for those risks and around risk management itself. These are summarised below:

1. Outsourcing makes life easier with less to worry about as the responsibility for risk can be delegated to others

Whilst an authority may have delegated the delivery process, and even delegated the day to day risk management processes, the responsibility to meet statutory, in tort, political, contractual and other promises has not moved one inch. The further challenge is to bring the wider culture, political, reputational, regulatory, funding constraints and statutory responsibilities into a relationship with a third party who may not be familiar with these additional sensitivities.

A huge risk for a widely outsourced environment is of course the accumulation risk; whereby the failure of one supplier can simultaneously affect the authority in different departments and indeed can affect other, perceived to be separate, suppliers to the authority.

2. Once a relationship is created it will manage itself

Understanding and effectively controlling third parties’ risks takes the chief executive and staff well beyond erstwhile silos of risk management. They have in the past been able to consider independently the insurance needs, operational failure, financial risk, governance and legal risk, business continuity planning, project management, co-ordinated incident response, credit risk, and relationship management.

Effective supply chain risk management demands that these management silos are brought together to understand just how the holistic relationship and its outcomes expose the authority to failure.

The sheer scale of a relationship may mean that it is impossible to cancel it quickly and regain the ability to deliver back in-house. If so, the relationship needs actively to integrate the authority’s own risk management personnel and systems with the counterparty’s own staff and day to day control systems.

3. Spending time on an exit strategy is for wimps

All outsourcing where the relationship delivers critical services needs a trusted exit strategy that is pre-agreed by both parties. This exit strategy needs to recognise that circumstances may change, gradually or by sudden failure, and will enable the authority to quickly take back activity or be able to transfer it to another third party whilst continuing to maintain essential services. This is crucial amongst our messages and an entire section of this full Briefing Paper is devoted to this need.

The House of Commons Public Accounts Committee’s 2009 report, Central Government’s Management of Service Contracts, included the following findings:

The extent to which central government tests the value for money of ongoing services and contract changes is variable. For example:

- 41% of contract managers had not tested the value for money of new services purchased under an existing contract
- Planning and governance is one of the weaker areas of contract management, although there are examples of good senior level engagement
- Less than half the organisations surveyed had an individual with overall responsibility for contract management
- There was no documented plan for managing 28% of contracts
- 56% of contracts did not have a contingency plan in case of supplier failure
- 30% of contracts where suppliers were dealing with personal or security information did not have a risk register
- No commercial director/head of procurement rated the level of resources allocated to the management of their major contracts as ‘good’
“Expertise seems to be in short supply and at the centre it is fragmented across several agencies. In particular, there is a need for greater expertise in …… constructing effective partnerships with the private sector.”

The Lyons Report 2004; 1.21

4. Charities and Third Sector (civil society) organisations are easier to handle
Large private sector companies may have the experience, skills and lawyers to set legal relationships that will absorb them from some of the consequences of failure. On the other hand some charities may not have the skills to critically understand their risk of failure; nor the ability to react to threatening incidents. They may need considerable additional support and investment to bring their risk understanding and resilience up to the authority’s minimum standards; without this they are likely to be brittle and quickly exposed to complete failure.

It is for this reason that an entire section of the Briefing Paper is devoted to the additional challenges and opportunities of using third sector organisations as contractors and partners.

5. No new skills are required to manage an outsourcing delivery
Understanding and dealing with the much more amorphous and long term risk of a third party’s failure sets new and increasingly difficult challenges for public service employees that are beyond their historical experiences and comfort zones.

Many Risk Managers have in the past been charged with simply managing financial risk through insurance products. Their role not only needs to be significantly widened but the chief executive and the authority have a responsibility to ensure that these new challenges in risk management are adequately skilled and resourced.

6. Due diligence enquiries provide all the answers
Sadly, there are no handrails. Lawyers and accountants will indeed advise on the legality and finances of a project proposal. Choosing whether outsourcing is the right way forward, and if so with whom, needs much wider and deeper consideration.

Decision making around tenders needs to be risk-weighted and not just based on price. Price auctions, in whatever form, are very dangerous without clarity on the service level compromises proposed at each price. This is especially important of course in sensitive, mission critical services such as social care of vulnerable people. Project managers, at any stage of the project, may need to suggest that the entire project should be withdrawn or reconsidered; or that any changes to the outcomes need to be risk managed again. Above all, any consultation needs to be a genuine urge to listen to stakeholder views and not be used simply to engineer acceptance.

Too often short term, accountant-measured, cost savings can become future years’ cost overruns, failures and even disasters if the more difficult cost of risk and off-balance sheet liabilities are not measured and brought into the decision making. Any political expediencies need to be managed and not become a reason for bypassing sound operational and long-term outcomes and cost considerations. The bottom line will always be: is this right for us, for our operations, our ethics, our cultures, comfort alongside our other operations, our long-term risk tolerances, and above all, our community?

7. You can best risk manage outsourcing risk once the relationship has been created
The only fully effective risk management of third party failure is at the time that the relationship is created. The very design of the relationship needs to be risk-aware; and that all risks arising, now and into the future, will be communicated and remain firmly within the authority’s risk comfort levels. It is far too late to consider risk once contracts have been signed.

There is need for realism amongst officials and their sponsors to accept that, however carefully the project is created, it could still fail or need to change; and that they need to retain the ability to manage that change; and, if necessary, successfully achieve a closure of the relationship.

Big is not always beautiful and can bring risks in itself. This can only be possible if an alternate market is retained in the product or service. Co-operation between authorities can in effect force a monolithic market place of suppliers that may give short-term gains but close down future opportunities to spread risk.

8. Information is less important than the things you can touch
Information, and the ability to mine that information, is at the heart of modern day business models. Massive amounts of this information can be stored in tiny hardware tools from CDs and laptops to hard drives and USB drives. Losing the ability to access that information can instantly bring the whole organisation to a halt. Authorities cannot complain however where they have not set those standards and ensured that the information holder is clearly aware of their importance.

9. We don’t need risk management, we have insurance
The greatest damage is unlikely to be just financial; but can, crucially, be when there is a failure to deliver on responsibilities. Insurance products, often the sole agenda in the past of risk managers, remain vital for managing financial exposures. The very nature of modern day business models however means that this is now a part of a much wider need for identifying all endemic risks and impacts; and managing them down to acceptable levels.

This calls for reconsideration of the role and skill levels of some employees currently described as Risk Manager.
1.5 Key questions for local authority leaders

Below are some of the key questions that local authority executives could usefully be asking in supply chain outsourcing arrangements:

• Does the chief executive officer understand that the responsibility for risks and resilience in service delivery rests with that role and cannot be delegated, neither internally nor externally?
• Is the supply chain project sponsorship at the correct and suitably skilled level; and is there a clear, senior level owner of the overall responsibility for risk?
• Does the project design require outcomes that include report on risks within any new framework that is being proposed; and also any new risks that may be introduced into other parts of the organisation?
• Does the project design brief demand an exit strategy and plan?
• Do risk registers embrace the potential loss of intellectual and other assets, losing control over the process itself, data privacy, potential loss of quality of service, ability to communicate, the ability to remain legal, and threats to confidence and reputation?
• Are the supply chain project managers skilled, resourced, or supported adequately to respond to the challenge of understanding outsourcing risk and its effective management? Are they in particular aware of the authority’s sensitivities and risk tolerance limits?
• Do the tendering and decision processes actively and consistently expose risks within each of the tenders and ensure that the choice of counterparty is formally risk-assessed?
• Does the project brief demand that the deliverer of services has adequate risk processes; including resilience plans that embrace the authority’s own urgencies and sensitivities?
• Are outsourced service promises and liabilities embraced within routine control and governance procedures?
• Does the authority’s risk controls embrace important non-financial exposures as well as the financial ones?
• Do the project managers and their sponsors feel comfortable that if they find that unacceptable exposures have evolved that they can suggest that the project may be closed or that at least, some fundamentals need to be reconsidered?

1.6 Summary

In a nutshell, the outsourced business model is much leaner and has much less margin for error. Its ability to absorb surprises is gone for ever, and thus understanding and managing its risks has never been more critical.

Outsourcing a supply chain critical service need is so much more than subcontracting. Contracts may be tiny or huge. They can range from ones that embrace emergency services to emptying dustbins to the management of a community hall. As such, they all demand different levels of risk attention. The priority however is not determined by the size of the contract but: how much harm will a failure cause? The responsibilities of the public sector, and the consequences of failure, are diverse, serious and wide-ranging. Authorities not only have contractual and legal responsibilities in tort, but crucial statutory and political responsibilities too and these responsibilities crucially need to be embraced by the chosen partner organisation.

The Briefing Paper sets out to support the authority in meeting its responsibilities and the secure delivery of its Local Area Agreement as measured through the Comprehensive Area Assessment; and whilst risk aware management is simply no more than good management, also to satisfy its Statutory, Audit, and other Governance requirements.

As a starting point the chief executive may wish to appoint a senior governance, strategic or risk director to explore the current situation within the authority, prompted in part by the key questions for leaders.
1.7 Objectives of the Briefing Paper

The Briefing Paper sets out, in a practical way, to support chief executives, politicians, auditors and their authorities in meeting these new and testing challenges. The Briefing Paper deals with the particular challenges of delivering crucial responsibilities through large and small contracts with third party providers and also by less informal partnership working.

The paper recognises that there are variations across England, Scotland, Wales and Northern Ireland but the principles, whilst necessarily generalised will, we believe, be of value to all local authorities and all areas.

Managing risk when core responsibilities have been outsourced to a charity or other third sector organisation is covered in its own separate section in the Briefing Paper. This sets out not only to raise, realistically, the additional challenges that they bring, but also to illustrate where effective risk management can enable such a relationship, when it is preferred policy, to become achievable.

As stated in the Orange Book: Management of Risk – Principles and Concepts (2004) we set out in the paper to bring practical advice and prompts to:

- those who are new to risk management and those who are tasked with providing training on risk management in their organisations, both of whom will find it useful as a key introductory document
- those who are concerned with the review of risk management arrangements (such as Audit Committees) as a resource providing a comprehensive statement of principles against which actual risk management processes can be evaluated
- senior staff whose leadership is vital if an appropriate culture is to be generated in which risk management can be effective
- operational level staff who manage day to day risks in the delivery of the organisation’s objectives and who will find it a practical support in the actual management of risk; and those who are experienced in risk management, for whom this guidance explores more difficult concepts such as risk appetite

It will be equally of use whether the reader’s focus of interest is with managing risk at strategic, programme or operational levels.

2. The new world of outsourcing and its implications

2.1 Outsourcing; its values and threats

Outsourcing and partnership working is not new. Beveridge believed in 1948 that the State should take the lead in slaying the “five giants of want, disease, squalor, ignorance and idleness,” but believed that “it could not do it alone.”

Local authorities are dramatically increasing their use of third parties to deliver on their statutory and other responsibilities. This operational model now lies at the very heart of the way the public sector meets it responsibilities and how it is planning to do so.

The move to outsourcing has long moved on from just a way to reduce cost. It is now as much about taking opportunities through entirely new operational models that are much more focused, efficient and have a better ability to differentiate between suppliers and between individual service users. It is a way for authorities to focus on their core strengths and to use the expertise and resources of others to carry out the functions they may not be as well equipped to perform. It enables authorities to focus on their leadership responsibilities while retaining focus on the core values of cost and quality of service. Furthermore, when risk-managed effectively, outsourced delivery can carry less, not more, risk of failure.

Audit Scotland acknowledges the outsourcing and partnership working shift in their paper, Priorities and Risks Frameworks (2006/9):

“52. To promote the links described above between the Priorities and Risks Framework (PRF) and other work, we have set out this year’s PRF under headings that reflect those we are using to develop the corporate assessment for Best Value 2 (BV2) (Exhibit 1).

As such, the section headings are:

- Vision and strategic direction
- Partnership Working and Community Leadership / Engagement
- Governance and Accountability
- Performance management and improvement
- Risk management
- Use of resources (financial management; people management; asset management; procurement; Information management)
- Service priorities and risks

…Our vision is of revitalised local authorities, working with their partners, to reshape public services around the citizens and communities that use them.

…The new regime – Comprehensive Area Assessment – will be a more proportionate risk-based regime which will cut bureaucracy and allow more targeted support or intervention when things go wrong.”

Strong and Prosperous Communities.
The Local Government White Paper 2006
Similarly, The Local Vision Statutory Guidance from the Welsh Assembly Government on developing and delivering community strategies, 2008 includes the statement: “The community strategy is the overarching strategy for each local authority area. Local authorities have a community leadership role, but the strategy should belong to the community, and should be prepared and implemented by the local authority in conjunction with its public, private and third sector partners.”

Responsibilities remain firmly with the authority. The risk is now much more difficult to understand and control. Only if there is a consistent measurement of risk and potential damage can informed decisions be made about whether a risk being carried is an acceptable one or not. The authority cannot turn its back on the risks assumed by the counterparty when and after accepting the contract. Its failure will also be the authority’s failure.

There are countless lists of outsourcing key risks but here is just one of them:

- Partner or supplier underperformance
- Governance
- Hidden costs & cost budget overruns
- Potential loss of knowledge, intellectual property and other assets
- Data privacy issues
- Losing control over the service itself
- Potential loss of quality of service
- The ability to remain legal
- Threats to reputation

Calling a Change in the Outsourcing Market. Deloitte Consulting LLP 2005

Sobering thoughts emerge from survey after survey and from very public failures when strategic outcomes have failed and costs have exceeded budgets by many times. Reputations have too often been shredded when the media has picked up on failures to protect and secure stakeholder interests and sensitivities. In just one piece of research by Gartner (2005), responders reported that the failure rate of outsourcing contracts to meet expectations is fully 50%.

Outsourcing is therefore no longer a bolt-on management tool, but an everyday way of life, at the very heart of operations at local, regional, national and global levels.

Managing third parties that have different agendas, think differently and above all have different cultures and attitudes to risk can however be the greatest challenge now facing authorities.

This is clearly a private sector view too. In an FM Global survey in 2005, supply chain worries topped the list of risks causing major disruption.

If we need further evidence of the need to develop outsourcing risk management, we can refer to the House of Commons Public Accounts Committee’s 2009 report, Central Government’s Management of Service Contracts, which includes the following findings:

- The extent to which central government tests the value for money of ongoing services and contract changes is variable
- 41% of contract managers had not tested the value for money of new services purchased under an existing contract
- There was no documented plan for managing 38% of contracts
- 56% of contracts did not have a contingency plan in case of supplier failure
- 30% of contracts where suppliers were dealing with personal or security information did not have a risk register
- 22% of contract managers considered they did not have time to perform their responsibilities well

Public authorities have unique and difficult challenges, more so than profit-making companies. They have critical responsibilities that go well beyond profits and asset protection. Their outcome expectations demand immediacy and resilience; often 365 days a year and 24 hours a day. Many of these outcomes are linked to community safety and life-threatening situations, include vulnerable service users and demand instant responses to emergencies and other fast changing situations. These responsibilities continue undiminished during periods of concurrent structural change, remain during difficult economic conditions, and always need to be delivered within a framework of best value.
2.2 What is supply chain management?

Typical supply or delivery chains are described in the table opposite, illustrating the very wide range of formats available to an authority.

Each of these formats has different risks and can cause quite different types of failure.

For example: a shared service operation has a greater accumulation risk where one failure simultaneously creates damage to separate and important providers.

Furthermore some causes of failure such as severe weather, flooding, pandemic, lack of bankers’ availability of working capital, and employee unrest can affect different organisations simultaneously. If that is not enough, we also need to remember that the first level supplier to the authority may be dependent in turn on mission critical services delivered to them by their own outsourced suppliers, within the UK and overseas.

Risk management is not just an operational management issue. It is equally at the heart of strategic management and begins at the very first thought of: “Should we outsource, and if so for what reasons, values and objectives?” The cost/benefit analyses cannot work if they only measure current revenue costs and gains.

Cost and benefit measures need to include the values of confidence, the need to remain in control, resilience, reputation, continuing legality, trusted management information, and flexibility. Putting a cost and value on any short term and long term risk needs to be included; also required is the cost of any governance, support and control procedures needed to ensure risk awareness at all times. These control procedures need to recognise that open and fully frank communications may be difficult with a third party that may wish to hide or delay the disclosure of their problems to an important customer.

When the outsourced division is very large, a quick pull back is just not achievable.

The authority must, before the signing of the contract, ensure that its own risk management processes and standards are embedded right across the service or outcome delivery, and will constantly work alongside those of the supplier; with the power to introduce change if the risk profile becomes unacceptable.

All this will be at a cost that needs to be factored into the initial decision of: “Should we outsource, and if so for what reasons, values and objectives?”

### Types of Local Authority Supply Chains

<table>
<thead>
<tr>
<th>Inbound – back office</th>
<th>Outbound – front office</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Corporative Services</strong></td>
<td><strong>Community Services</strong></td>
</tr>
<tr>
<td>Local Authority Internal Resources</td>
<td>Local Authority Service Delivery</td>
</tr>
<tr>
<td>• Authority assets &amp; functions (premises, FTE)</td>
<td>• Authority assets &amp; functions (premises, FTE)</td>
</tr>
<tr>
<td>• Non-contracted</td>
<td>• Non-contracted</td>
</tr>
<tr>
<td>• Direct Labour Operations (DLO)</td>
<td>• Possible multi-site network</td>
</tr>
<tr>
<td><strong>Contracted Suppliers</strong></td>
<td><strong>Contracted Provider</strong></td>
</tr>
<tr>
<td>• Service contracted to third party supplier</td>
<td>• Service contracted to third party supplier</td>
</tr>
<tr>
<td>• Third party may sub-contract to additional subcontractors</td>
<td>• Possible subcontracting</td>
</tr>
<tr>
<td><strong>Shared Service Operation</strong></td>
<td><strong>Shared Service Delivery</strong></td>
</tr>
<tr>
<td>• Centralised back office admin or centralised service</td>
<td>• Front office service delivery</td>
</tr>
<tr>
<td>• Based on lead authority</td>
<td>• Based on lead authority (e.g. Waste disposal/ Housing benefits)</td>
</tr>
<tr>
<td><strong>Outsourcing Arrangements</strong></td>
<td><strong>Joint Venture/PFI Arrangements</strong></td>
</tr>
<tr>
<td>• Risk control may not transfer</td>
<td>• Risk control may not transfer</td>
</tr>
<tr>
<td>• Authority retains some ultimate liability</td>
<td>• Authority retains some ultimate liability</td>
</tr>
<tr>
<td>• Significant outsourcer</td>
<td>• Theme or special scenario (Education)</td>
</tr>
<tr>
<td><strong>Partnership Working Network</strong></td>
<td><strong>Partnership Working Network</strong></td>
</tr>
<tr>
<td>• Service supplied by third parties on non-contract basis</td>
<td>• Service delivered by third parties on non-contract basis</td>
</tr>
</tbody>
</table>

Source: Zurich Municipal ©
A New World of Risk

These relationships are often controlled solely by contract wordings designed with no thought of failure, change or separation. There are special exposures when partnership working with other departments and with the third sector. These responsibilities may be passed into informal, more amorphic, partnerships without the discipline of formality and can bring even greater surprises and failures. We return to these additional concerns later in the paper.

Risk is also not only about the moment when there has been a failure to deliver. Every organisation has a range of core dependencies without which it cannot possibly recover from any failure or loss. In the process of outsourcing, these dependencies have often been passed over to third parties and need to be recovered, in a useable format, if there is any chance of reinstatement of service in time to meet any critical and especially urgent needs.

Transferred divisions of the authority will have any critical and especially urgent needs. They may have very few spare resources and the skills to understand their own risk of failure. Some local authority partners may not even have financial and reputational relationships that will favour them when things go wrong. Conversely, any critical and especially urgent needs.

2.3 Management skills

There is an even further challenge and it is a crucial one. Outsourcing takes the authority’s existing employees into areas of responsibility where they may feel less experienced and skilled.

Outsourcing now brings the authority’s partners’ business risks right into the forefront of an authority’s own ability to deliver promises. Examples would be the failure of the partner’s continuity management, insolvency, competitor activity, succession planning and availability of working finance, not least the foundations needed to sustain long-term Public Finance Investment (PFI) initiatives.

Many a 21st century private sector partner can itself be described as a ‘hollow company’; where its own delivery is supplied by third parties under contract. The risk profile of the partner is now equally the risk profile of any authority that employs them to deliver on its own critical responsibilities.

Apart from the skills gap, understanding a third party’s risks has to be much more amorphic. Private sector companies may have the experience, skills and lawyers to set the legal, financial and reputational relationships that will favour them when things go wrong. Conversely, some local authority partners may not even have the skills to understand their own risk of failure.

They may have very few spare resources and money to react effectively to organisation-threatening incidents.

2.4 Does the organisation manage its risks and maintain a sound system of internal control?

This individual KLOE has a focus statement, which requires that: “the organisation has effective risk management that covers partnership working.”

CAA – Key Line of Enquiry

KLOE: 2.4 Does the organisation manage its risks and maintain a sound system of internal control?

There is an even further challenge and it is a crucial one. Outsourcing takes the authority’s existing employees into areas of responsibility where they may feel less experienced and skilled.

Outsourcing now brings the authority’s partners’ business risks right into the forefront of an authority’s own ability to deliver promises.

Examples would be the failure of the partner’s continuity management, insolvency, competitor activity, succession planning and availability of working finance, not least the foundations needed to sustain long-term Public Finance Investment (PFI) initiatives.

Many a 21st century private sector partner can itself be described as a ‘hollow company’, where its own delivery is supplied by third parties under contract. The risk profile of the partner is now equally the risk profile of any authority that employs them to deliver on its own critical responsibilities.

As always, crossing organisational boundaries brings its own co-operation and communication walls to climb. It will call for some authorities to reconsider the role of risk officer and ensure that it becomes positioned, resourced and skilled adequately to face these new challenges.

Technicalities apart, designing a resilient relationship demands modesty amongst officials. However carefully the project is created, it could still fail or need to change. This takes the politicians, chief officers, risk managers, project managers and strategic managers to admit that withdrawal may be needed at some time in the future and that such withdrawal will need to be planned, agreed and resourced now, if urgent services are to continue effectively. A section of this paper is dedicated to exit strategies.
2.4 Reputational risks

Randolph Hearst is quoted as saying that “News is something someone doesn’t want to see in print. All the rest is advertising.”

With the modern day, intensively competitive, 24-hour news media, no paper on organisational risk should omit a section on the importance of reputational risks. Not only do the organisation and its chief executive need to deliver as promised, but they also need to retain at all times the confidence that it will continue to do so. A public service may not have a long line of competitors ready to leap in and steal customers but the importance of trust is no less critical. A distrusting service user creates a greater resource challenge than one who is comfortable. Fund holders and financiers, regulators, partners and suppliers in all their formats will also need to remain assured of the authority’s ability to deliver. Retaining and attracting the best employees is very much a reputational issue.

Above all, a local authority needs to be trusted by its community if it is to stand a chance of delivering in its core role as a ‘place shaper’ or leader in the community planning partnership.

A media attack diverts resources massively and creates its own chain of events. All this can happen during a crisis that needs all the available resources to hand. Routine risk management prepares media conference rooms, dedicated websites, satellite phones, press conferences and dedicated media lines in case the media interest is large scale and international. These resources need to be available continually and have access to the latest information as it emerges. Precise and urgent instructions or messages should be circulated to avoid unauthorised, possibly incorrect, information being released by staff or others. However, all this is made pointless if counterparties push forward their own brand protection strategies at the expense of the authority.

2.5 Getting the design of the relationship right the first time

If the fundamental design of the partnership is wrong, then the relationship will fail; and no amount of post contract risk management can be fully effective.

Tendering decisions need to be risk-weighted and not just based on price.

Crucially, at every stage project managers should feel comfortable reporting back that they have discovered that the project’s proposed delivery methods have become too risky and the entire project should be withdrawn and reconsidered. Subsequent drifts in the project’s initial objectives present entirely new risks to manage. Above all, any consultation needs to be a genuine urge to listen to stakeholder views and not be used simply to engineer acceptance.

Outsourcing and partnership models enable the organisation itself to upscale and downsize much easier and more quickly than before, and thus offer opportunities to spread risk and manage a crisis. A diverse supply chain can therefore be a useful way of spreading risk as well as a way of concentrating risk into single, potentially catastrophic, failure points.

Outsourcing is so much more than subcontracting. It creates greater challenges in understanding third party risks; and yet can bring valuable risk management opportunities.
3. The risk management toolbox

3.1 Risk objectives and role

Ensuring risk awareness and then resilience is not, of course, a separate branch of the generic management task. It is simply good management. Satisfying Government guidelines, not least Audit Commission requirements, is not the primary objective here – but simply a by-product of good management. We therefore begin this section with an urge that outsourcing risk controls are not separated but fully remain within the overall strategies, governance procedures, controls, risk registers, tools, and cultures of the home organisation.

The ALARM survey of 2006 confirmed that risk management is increasingly used to contribute to objectives, delivery, targeting of resources and improving service delivery.

The role of the risk officer is to carefully advise the most senior decision makers so that they can make the best informed decisions about risk; the acceptance or otherwise of those risks. This professional’s grasp of risks must embrace a clear understanding of the authority’s responsibilities and outcomes.

Surveys have placed Damage to Reputation, Business Interruption, Third Party Liability, and Disruption or Supply Chain Failure at the very top of risk concerns. We suggest that each and every one of these concerns is a supply chain issue.

‘Off-balance sheet’ responsibilities may be statutory ones, in tort, criminal or other legalities, in safety, security, environmental, or just simply to meet each and every one of the confidences that individual stakeholders have in the organisation. The responsibility equally is to be able to satisfy audit, regulatory and media challenges.

Managing supply chains brings particular challenges, but there are also important ones in common with the risk management challenges of older business models. In recognising and needing to work here on the differences, it is important that we do not lose sight of basic commonalities.

The first and underlying fundamental is that organisations still need to understand and measure risks in a consistent way right across the organisation. All organisations exist for the benefit of their stakeholders. Even though these stakeholders can be different, organisation by organisation, whether public, private or third sector, their interests and expectations need to remain at the heart of any risk strategy. When an organisation asks itself “What is my tolerance to risk?” the real question is “What is the tolerance to risk of my service users and other stakeholders?”
3.2 The tools available

Once a risk manager has identified and quantified the risk of failure, and then the potential consequences to stakeholders of that failure, the normal risk management toolbox begins to provide six headline options to respond:

The risk management tools:
1. Accept both the risk and the impact
2. Reduce the risk down to tolerable levels
3. Reduce the potential impact down to tolerable levels
4. Transfer the risk to a third party
5. Prepare financial plans to enable any monetary cost to be funded
6. Prepare so that the strengths and resources of the organisation can be used to manage an incident and contain its impact within acceptable levels

3.2.1 Accept both the risk and impact

The local authority may decide that the worst-case scenario is one that does not result in unacceptable damage. It will therefore make a formal and documented decision that the risk and the potential consequence of the particular delivery chain failure is acceptable. If this decision is not possible, doing nothing is not an option. The local authority will need to move on to one or a combination of the other tools available.

Clearly it also needs to ensure, by use of its governance and change controls, that the risk does not subsequently move to an unacceptable level.

3.2.2 Reduce the risk down to tolerable levels

The decision may be to remove the organisation from an activity or responsibility because the risks from that activity are unacceptable, or the cost of managing those risks is too high. It could be of course that outsourcing, or at least outsourcing into the available marketplace, cannot be done safely. The authority may especially take a hard look at any promises they may wish to make to their public and ask first: are they actually achievable as described?

3.2.3 Reduce the potential impact down to tolerable levels

The risk manager will also look at the potential impact of a risk to the responsibilities and outcomes that the local authority have assumed and then take steps to control that impact. An obvious example is to secure tightly, and back up, electronic data frequently; and instantly store that back up data well away from the primary risk site. Even this would not be of value if it does not include any hardware, software, human resources, communication tools and workstations that will enable it to be used fast enough and effectively.

Table Urgency and Alternatives

<table>
<thead>
<tr>
<th>Speed required</th>
<th>Alternatives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Immediate dependency</td>
<td>Not available elsewhere in volume, quality and quickly enough.</td>
</tr>
<tr>
<td>Immediate dependency</td>
<td>Available elsewhere in volume, quality and quickly enough.</td>
</tr>
<tr>
<td>Mid-term dependency</td>
<td>Not available elsewhere in volume, quality and quickly enough.</td>
</tr>
<tr>
<td>Mid-term dependency</td>
<td>Available elsewhere in volume, quality and quickly enough.</td>
</tr>
<tr>
<td>Non-urgent dependency</td>
<td>Not available elsewhere in volume, quality and quickly enough.</td>
</tr>
<tr>
<td>Non-urgent dependency</td>
<td>Available elsewhere in volume, quality and quickly enough?</td>
</tr>
</tbody>
</table>
There may indeed be a way of delivering services at lowest cost, a measure beloved of accountants, but risk management investment lies at the very heart of the value of the relationships as well as at the cost of the relationships.

A widget, for example, may be available at a cost of 20p each by using purchasing power to drive down the cost from one exclusive supplier. The authority may however decide to purchase widgets from two or more independent sources, forgoing some of that volume purchasing power. Should the cost now be 30p each, that additional cost of 10p per widget can, when subjected to a risk assessed cost benefit analysis, be an effective risk management investment. Driving down the cost of care of vulnerable older people by online price auction is a clear and dangerous public authority and service delivery equivalent.

Furthermore, by co-operation with other authorities, the huge purchasing power may drive one significant player to deliver cheaply, but at the same time the single contract could destroy the viability of competitors to that business. The resultant dependency on one monopolistic supplier may in itself become an unacceptable risk.

The public sector is unable to relax in the confidence that their customers cannot move to competitors. The example below illustrates that contracts may be removed from public service organisations, and increasingly so in the new environment.

“Directors of Heart of England Tourist Board have decided not to continue trading beyond the end of this financial year.”

Tourist Board chief executive, David Moyser, said “Advantage West Midlands, the regional development agency, had decided not to renew its contract with Heart of England to deliver a range of regional tourism marketing and support activities.”

The Gloucestershire Citizen, June 2007

Clearly, this confidence in lack of competition can no longer be true and it is also the customer’s reaction to a perceived and real failure that can turn a problem into a disaster. Just one example was the huge number of people contacting the Passport Authority when delays in issuing passports caused them to panic that their passport would not be delivered in time for their trip.

It can be useful to consider who, from a risk dimension, these stakeholders are. With a focus on the public sector, they include:

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Expectations</th>
</tr>
</thead>
</table>
| Employees   | • Morale and pride in what they do in the organisation they work for  
              • A safe working environment  
              • Confidentiality in the personal information that they have shared |
| Customers and service recipients | • To receive the service promised; often services that are crucial, extremely urgent and potentially lifesaving to people who at the time are in the most dire of personal circumstances  
                                         • Confidentiality in the personal information that they have shared |
| Funding     | • To deliver on the promises that have been made to the providers; whether they be Government bodies, partnerships, contracted responsibilities, or private sector sources of funds |
| Suppliers of services | • Suppliers have a legal contract to deliver to the authority  
                              • The supplier is additionally a stakeholder, in that should the principal fail to meet expectations (or simply cause it to fear that it will fail to do so) the supplier may withdraw its own service delivery |
| Partners    | • In many ways partners bring the same risk as suppliers but a less formal contractual arrangement may make it much more difficult to recover smoothly from a crisis situation |
| The environment | • There is also the crucial importance of retaining trust in the political, natural, legal and democratic environment; whether that is at national, regional or local level. In addition to the authority’s own responses, the Civil Contingencies Act 2004 calls for important emergency community dependencies |
| The media   | • By the very nature of the responsibilities that public service carries, a local authority is constantly in the media spotlight. The media can effectively be described as wholesale creators or destroyers of reputations and trust |
### 3.2.4 Transfer the risk to a third party

Often, a lawyer will indicate that the contract wording imposes all the risk on the counterparty. However, if the counterparty is delivering a critical and urgent service, the failure of that counterparty will itself create a potential failure of the authority’s own responsibilities.

### 3.2.5 Prepare financial plans to enable any monetary cost to be funded

Spreading loss, perhaps by spreading the cost over a longer period of time, is useful but necessarily can only provide loss protection when that loss is a financial one. It is useful to remember that many of the most devastating damages are not caused by financial loss. Moving urgently from one supplier to another may incur unexpected costs, for example, and should be built into financial contingency plans.

### 3.2.6 Prepare so that the strengths and resources of the organisation can be used to manage through an incident, containing impact down to acceptable levels

The sixth tool within the toolbox can also be called business continuity planning or resilience management and includes precisely the form of business continuity management that is the subject of British Standard BS25999 Business Continuity Management. The work described by this standard and others is immensely valuable but is by no means the whole story. Again there is a section in this paper bringing out hidden minefields for consideration (see Section 4 – Myths and opportunities). It is worthy of mention now that, however carefully such a programme can be created, the supplier may still fail; or indeed its own business continuity plans may not take the authority’s own sensitivities, responsibilities, urgencies nor needs into account.

Where the workforce is employed by another legal entity, the ability to micro-manage and redirect them to meet an urgent new challenge may be lost or at least severely diminished. This is not least when the supplier is simultaneously contracted to also deliver services to its other customers.

It is often not achievable for business continuity programmes to restate all services immediately. Plans are based around a business impact analysis, which, inter alia, agree with front line managers beforehand the absolute minimum service levels (MSL) they need to deliver urgent and critical services whilst a full rebuild is under way. Very rarely do we see these MSLs built into contracts with third party suppliers.

### 3.2.7 Understand current dependencies

The underlying principles of the risk manager’s toolbox, enabling both opportunities and threats, remain valid for use even through the applications can be very different in addressing supply chain and individual public service exposures.

### 4. Myths and opportunities

#### 4.1 Background to the section

This section of the paper considers some common myths, minefields and opportunities within outsourced supply chain delivery. They are not listed in any particular order of importance.

### Myth 1: Outsourcing makes life easier with less to worry about

It is worth raising again here, as a myth, a subject we have raised before; the myth that outsourcing is the same as subcontracting, and it is crucial that this delusion is removed if the risks are to be understood. Outsourcing does so much more than require a third party to deliver a piece of work; as an entire section or sections of an organisation is being handed over to another legal entity.

The ability to continue to deliver through these organisationally narrow routes, and the raised expectations, have equally become critical dependencies. The modern day risk manager may have, numerically, fewer worry beads than in older in-house delivery models, but failure in any one of them has the potential, not only to damage, but to destroy an entire organisation.

All this has shifted dramatically the Achilles heels of these organisations; and equally the new services and speeds now promised to stakeholders have raised expectations way beyond previously recognisable levels.

Stakeholders now expect simultaneous access to their personal information, immediate answers to their questions and instantaneous delivery of the product or service required.

Again, the decision to outsource therefore is also a decision to pass these crucial dependencies over to third parties who have different agendas, different stakeholder pressures to satisfy, different governance standards, attitudes to risk, varying levels of resources to apply to risk management, and very different attitudes and cultures. Getting the dependencies back is not easy, and when needed the process may have to overcome operational, human, technical, legal and practical problems that could, if achievable at all, in the meantime stop delivery of crucial and urgent services.

The opportunity is to position right from the beginning the skills, contracts and processes that will enable the authority to gain access at all times to information that will enable them to understand the risks being carried, and to then do something about them.
A New World of Risk

Myth 1a: The responsibility for risk can be delegated or passed to others

The day to day function of risk management realistically must often be delegated but responsibility for failure cannot be so delegated. All risk-measured management therefore needs to include governance and control procedures to ensure that the organisation does not stray unknowingly beyond agreed risk tolerance now or at any time in the future. Imposing this control environment is the first responsibility of a chief executive; without which the job is unachievable.

As said, the chief executive’s and the authority’s responsibility is not at all diminished. This is made clear in the document Delivering Good Governance in Local Government (CIPFA 2007) when it specifically ‘makes a chief executive or equivalent responsible and accountable to the authority for all aspects of operational management.’ Obviously ‘all aspects’ must embrace outsourced responsibilities equally with those delivered from within. When a responsibility is outsourced, it is even more focused and can effectively be summarised as:

- The effective and risk-aware creation of the relationship
- The retention of statutory responsibilities and in tort
- Ensuring effective monitoring, risk information and audits
- Constantly retaining the ability to be flexible and to manage change
- Ensuring that there is the ability to exit or change as necessary whilst maintaining responsibilities and the delivery of critical services

A routine but important risk management guideline for an authority is to ensure that the workforce is fit for purpose by careful recruitment, behaviour controls, training and supervision. Where the employees are contracted to the counterparty, this responsibility remains; yet that counterparty may not have the same culture of risk aversion or care. Again, the need for this care must be embraced, in potentially sensitive areas, in the contracts between the authority and its suppliers; together with the ability to monitor such practices, for example: a health authority had outsourced emergency ambulance services but the drivers were found to be untrained and ill-equipped for the role.

There may be of course an opportunity for the authority to recover any losses that it has incurred caused initially by the failure of a counterparty. That ability to recover may be constrained by the wording of the contract between them; and also, realistically, the recovery can only fully be in respect of any financial loss. Other damages such as the loss of trust, reputation or in some cases the consequences of failing to meet a statutory liability are unlikely to be measured in such a way as to be a good basis for legal recovery.

The authority may be a litigant itself; or, as example: a health authority had outsourced the provision of emergency ambulance services but the drivers found to be untrained and ill-equipped for the role. A routine but important risk management guideline for an authority is to ensure that the workforce is fit for purpose by careful recruitment, behaviour controls, training and supervision. Where the employees are contracted to the counterparty, this responsibility remains; yet that counterparty may not have the same culture of risk aversion or care. Again, the need for this care must be embraced, in potentially sensitive areas, in the contracts between the authority and its suppliers; together with the ability to monitor such practices, for example: a health authority had outsourced emergency ambulance services but the drivers were found to be untrained and ill-equipped for the role.

A limitation period for a public authority to recover any losses that it has incurred caused initially by the failure of a counterparty may be constrained by the wording of the contract between them; and also, realistically, the recovery can only fully be in respect of any financial loss. Other damages such as the loss of trust, reputation or in some cases the consequences of failing to meet a statutory liability are unlikely to be measured in such a way as to be a good basis for legal recovery.

The Limitation Act 1980 will limit the time when such a recovery action can succeed to six years after the principal claim (or for personal injury, three years). It is crucial to remember however, that this limitation period will not begin until the claimant knows of ‘damage’, such as symptoms or the right to bring a claim. Some damage, such as asbestosis or sexual abuse in children’s homes, can mean that this evidence may be needed for many years beyond the Act’s headline limitation periods.

An Information Services Manager may, for example, have a view on information security controls. The only people however who can decide on those controls are those responsible for the delivery outcomes that emerge from that information and its sensitivity. It is only these front line managers who have a clear view, for example, of how often back-ups should be taken and removed, whether the information is critical enough to be encrypted, and whether passwords need to be changed.

Too often, disastrous loss of information has emerged because IS/IT managers have not been asked by, nor been told by, front line managers of the criticality of the information in their care. This needs effective communication and asking the right questions and it is a huge step further to bring this to the individual service suppliers that are employed by third parties.

Lawyers will confidently confirm that they have quoted a contract to ensure that risks have been passed legally to the counterparty. What this normally means is that, should the counterparty fail, the authority can sue them for financial compensation. This begs the most crucial of questions, “Just how useful is this, if the failure means that consequentially, the authority has itself already failed too?”

The balancing opportunity is to ensure that the responsibilities are understood clearly by all parties and that insurance and other protections are in place.
Myth 2: Once a relationship is created, it will manage itself

“There is little evidence that councils are using overview and scrutiny arrangements to hold LSPs, and partners, to account.”


This is one of the most dangerous myths of all. Often, the only guarantee that can be offered is that the visions will change. That change may be internal to the ownership, structure and management or personnel of either the supplier or the principal. There may be changes to the strategic objectives of either organisation or new opportunities may emerge that could have an impact on existing relationships. Any process of managing third party relationships therefore is very dangerous if there are no controls to ensure these changes are recognised, and any planned response remains achievable.

We have stressed that controls isolated from core operational control procedures are in themselves dangerous and, crucially, need to be embedded with the existing strategic controls. In an appendix we have made suggestions that can encourage the effectiveness of such control (see Appendix 1 – Embedding risk control procedures).

Once the relationship has been created it will need constant oversight and care. No amount of contractual clauses will, by themselves, keep the relationship on an even keel and the service delivered in quality and in time to the end of line service users.

A Risk Management Standard was developed jointly by AIRMIC, ALARM, and the IRM. This states this risk cycle well, as follows:

The British Standards Institution’s Public Available Specification 11000 focuses on the subject of Relationship Management. The specification calls for:

- The identification of one senior executive with the responsibility for collaboration and segmentation of the business relationships
- The clear identification and segmentation of existing business relationships; not least a clear understanding of their criticality
- The prioritisation of business relationships
- The risk assessment itself. This is where the supply chain risk and relationship risk comes alongside the authority's stated risk register and the activities that emerge from that risk register
- An understanding of the importance of both formal and informal relationships at all levels of employee within the organisations who are tasked with making it work

The relationships need always to have incentives to motivate each party at every stage; even during change and exit. Using purchasing power to bully suppliers into contractual submission is a clear route to failure in one way or another.

Disputes and problems are of course best understood and shared at an early stage when perhaps there may still be opportunities to resolve them and keep the supply flow moving without interruption. There is huge value in having a formal dispute resolution process that has been agreed at the outset by all parties. This will not only bring its own values when triggered but may encourage counterparties to raise concerns earlier and before irreversible damage is done.

Such a dispute process can identify who actually owns the problem, who addresses the problem and how.

The process can set out:

- Agreed early warning indicators
- How the problem and its causes are analysed; including access to information
- How the problem is assessed against individual and joint objectives
- The mediation process and its players
- The adoption of agreements and action plans
- The monitoring of the resolution agreed
- The measurements by which the problem is considered resolved
- Who is empowered to sign off the problem within each organisation

Furthermore, an arbitration clause may embrace:

- The designation by the parties of an actual person or company of professionals
- That whoever the arbitrator is, he/she must have experience and be qualified in the issues under dispute

There are a wide range of opportunities, as described above, to avoid this minefield.
Myth 3: Spending time on an exit strategy is for wimps

All outsourcing where the relationship delivers critical services needs a trusted exit strategy that is pre-agreed by both parties.

This exit strategy needs to recognise that circumstances may change, gradually or by sudden failure, and enable the Authority to quickly take back activity or be able to transfer it to another third party whilst continuing to maintain essential services.

This is crucial amongst our messages and an entire section of the paper is devoted to this need (see Section 6 – Exit Strategy).

Myth 4: Charities and civil society organisations are easier to handle

Large private sector companies may have the experience, skills and lawyers to set legal relationships that will absolve them from some of the consequences of failure. On the other hand, some charities may not have the skills to critically understand their risk of failure; nor the ability to react to threatening incidents. They may need considerable additional support and investment to bring their risk understanding and resilience up to the authority’s minimum standards; without which they are likely to be brittle and quickly exposed to complete failure.

It is for this reason that an entire section of the Briefing Paper is devoted to the additional challenges and opportunities of using civil society organisations as contractors and partners (see Section 5 – Partnering with the civil society – Its opportunities and additional challenges).

Myth 5: No new skills are required to manage outsourced service delivery

“Effective joint working needs active leadership and purposeful relationship management.”


When outsourcing, public service staff are brought into arenas that have been beyond their traditional experience. There are new barriers that make understanding risk more distant and thus more difficult.

- Planning and governance is one of the weaker areas of contract management, although there are examples of good senior level engagement
- Fewer than half the organisations surveyed, however, had an individual with overall responsibility for contract management
- No commercial director/head of procurement rated the level of resources allocated to the management of their major contracts as ‘good’

Central Government’s Management of Service House of Commons Public Accounts Committee 2009

It is difficult enough to take a measured view of all the financial and non-financial risks within one’s own organisation. Third party organisations have separate pressures, different stakeholders to satisfy and quite different minefields of their own to negotiate. Management controls, audits and the familiar risk management controls and standards are no longer available routinely as checkpoints. There may be reasons why a supplier will wish to conceal any weak points to an important customer until they have to.

The authority needs to consider carefully, before, not after, it passes crucial responsibilities to third parties, whether it has the right skills and experience available to make that relationship a success.

The National Audit Office commented that the delayed £513 million pound Ministry of Justice IT spend had doubled in cost. The report suggested that a former deputy chief executive “had responsibility for the scheme but had had little experience on big IT projects.”

The role and positioning of the risk officer or risk manager needs to be reviewed; not only in whether the key task objectives are sufficiently wide to take on non-financial and outsourcing risk, but whether the person yet has the strategic awareness, skills and confidence to embrace these additional exposures.
A further note of concern was raised:

“As a first step in developing a more sophisticated approach to supply chain management, it is important that a contracting authority understands its own capabilities in managing the supply chain. Whilst individual procurements and decisions on the make-up and management of the supply chain should be treated on a case-by-case basis, the authority must inform these decisions with an understanding of how well it is equipped to increase involvement and interactions with the supply chain, and also how well equipped its suppliers are to manage the supply chain.”

A New World of Risk

“Due diligence is...”

The due diligence process needs formally to understand precisely which dependencies have been outsourced, and, understand the importance, sensitivities and urgency of such dependencies.

The due diligence enquiry should also assess the achievability of the exit strategy (see Section 6 – The Exit Strategy).

In major projects, the organisation will structure its due diligence enquiries under different headings; and each may require different skills to deliver. These headings will embrace at least, the following:

- Financial models and sustainability
- Legality across all jurisdictions and compliance requirements
- Operational ability to deliver in time, volume, cost and to specification
- Quality Assurance; not just of the product itself but the branding and reputational consequences of how they are produced
- Quality sustainability
- Subjective due diligence

Subjective due diligence may be more amorphic but no less important. It is the one heading that cannot be delegated to professional advisers. This entails the authority standing back from the individual pieces of advice and asking “is this right for us?” In other words:

- Does this sit comfortably with our corporate vision, ethics, workforces and standards?
- Can we carry our communities and other stakeholders comfortably with this change?
- Are the risks of failure acceptable to us or otherwise manageable?
- Does the proposed partner’s culture and attitudes fit comfortably with our own?
- Do they share our own passions in stakeholder importance, our views on urgencies, and the acceptability or otherwise of failure?
- Are we able to stay in control of our responsibilities?

The subjective due diligence heading is, in effect, the helicopter view of all of the opportunities, the threats, strengths and weaknesses and enables the bottom-line decision whether or not to proceed. In 1999, Allan Leighton was Chief Executive of Asda and he and his team had decided on a merger with Kingfisher. After some months of working on this, he took the view that he was not comfortable that the chemistry between the two groups of people was going to work. No amount of hired due diligence specialist consultants could have come to that view; nor indeed should such a decision have been delegated to them.

There are serious dangers in relying on individual – focused due diligence enquiries. There is huge value from ensuring that, at the very highest level, there is a final helicopter responsibility for subjective value assessment.

These concerns around the importance and the adequacy of public service skills and experience have been echoed in a range of Government papers, including:

“The need for greater professionalisation in public sector procurement was recently highlighted in the National Audit Office’s (NAO) report on Central Civil Government procurement which found that:

- Most procurement is not carried out by designated procurement staff;
- Procurement staff are often consulted too late in the procurement process; and
- The majority of procurement staff do not hold professional qualifications’

Releasing resources to the front line. Independent Review of Public Sector Efficiency, OGC 2004

Myth 6: Due diligence enquiries provide all the answers

Authorities will undertake routine due diligence enquiries as part of the tendering process. Due diligence however is much more than ‘lawyers satisfying themselves about legalities; and accountants satisfying themselves that the figures add up. It is as much about becoming satisfied that the counterparty, overall and strategically, is fit for purpose.

The due diligence process needs formally to understand precisely which dependencies have been outsourced, and, understand the importance, sensitivities and urgency of such dependencies.

The due diligence enquiry should also assess the achievability of the exit strategy (see Section 6 – The Exit Strategy).

In major projects, the organisation will structure its due diligence enquiries under different headings; and each may require different skills to deliver. These headings will embrace at least, the following:

- Financial models and sustainability
- Legality across all jurisdictions and compliance requirements
- Operational ability to deliver in time, volume, cost and to specification
- Quality Assurance; not just of the product itself but the branding and reputational consequences of how they are produced
- Quality sustainability
- Subjective due diligence
A New World of Risk

Myth 7: You can best risk manage outsourcing risk once the relationship has been created

The decision to outsource is necessarily a sensitive matter, especially when a decision to do so could affect many employees who may lose their jobs or be transferred to another organisation where they may feel less comfortable. Informing and managing relationships with unions may need timely and careful communication. The downside of this is that too often the early work is done by a chosen few people behind closed doors; with professionals kept in the dark, ‘because they are not important enough to be included yet.’

With supply chain risk this danger is a very special one. Once a relationship has been agreed, choices, not least of any exit strategy, and the right to receive valid risk information and to integrate risk practices, may be lost forever.

In effect, the only time that risk and consequence can be fully addressed is at the time that the strategies are developed. Any risk management at any other time can only be peripheral to core risk and relationship management.

The standard project management textbook lists the drivers of time, cost, quality and scope. This misses a crucial one, not least in outsourcing projects, and that is risk. None of the other four drivers can possibly be truly assessed without knowing the risks that come with them.

Below is a checklist that may be useful when setting out to explore whether outsourcing is feasible:

- Financial models and sustainability
- Legality across all jurisdictions and compliance requirements; not least statutory obligations on authorities
- Operational ability to deliver on time, security, volume, cost margins, specification and within acceptable long term risk profiles
- Quality assurance, sustainability and checks
- Careful security management of people, information and other important authority responsibilities

There is always a danger that managers, fearful of the publicity around foreclosure of a public project will persist and try and make something work that is fundamentally flawed. Ongoing risk management controls fulfil the role of monitoring and advising in such circumstances.

Finally, in Appendix 4 (The 12 Strategic Questions, Audit Commission) we draw your attention to the 12 strategic questions proposed by the Audit Commission in the appendix to the paper Working Better Together; Delivery chain analysis, April 2009.

Myth 8: Information is less important than the things you can touch

Information, in all of its widest forms, deserves a section by itself in this paper. To do its part in service delivery it must be accurate, up to date, trusted, instantly accessible and useable, and often needs to be able to be mined instantly customer by customer, supplier by supplier.

Sensitive information in the wrong hands can cause immense concern and even actual harm; and can enable targeted terrorism and other crime. The responsibility that comes with holding information is therefore huge.

In the public domain there are huge and astonishingly expensive failures, for example in turning manual systems into electronic ones; and also where massive databases, packed into small laptops, USB drives or CDs have fallen into the wrong hands. The Department of Children, Schools and Families discovered in 2009 that there were security exposures around a £224 million ContactPoint database of vulnerable children. Is this an IT problem or a child protection problem? The reality of course is that it is both.

It goes without saying that where these databases are passed to third parties there should be a contracted and policed discipline in constant safety and security. It is obvious that these controls can only be inserted into a relationship by mutual agreement before contracts are signed.

Certainly the more sophisticated a system and its portability increases risk of failure. McKinsey in its 2009 research discovered that IT sophistication is not in equal proportion to added value:

Notably, our survey suggests that investments in formal IT systems (beyond basic enterprise-resource-planning ones) don’t improve supply chain performance as much as some managers expect. Companies relying more on spreadsheets and other informal solutions were nearly twice as likely to be inventory leaders—as likely to be cost leaders—and nearly three times as likely to be inventory leaders—as companies using formal IT systems extensively. That finding supports our view that they cannot replace strong processes, capabilities, and decision making. As one executive put it, “Our systems cannot be smarter than our colleagues, or we will have problems.”

This is a subject that could justify a paper in itself but we must restrict ourselves here to headlines only and stay within the context of outsourcing.

The key message is that there are real dangers in simply assuming that conventional insurance policies will transfer seamlessly when the cause of that stress is damage to the outsourcing contractor.

Simply making the counterparty a joint insured has its dangers too, not least because if that counterparty fails to meet any of the policy requirements or fails to disclose material facts, then the entire policy is void. Furthermore, any claims for failure between the two policyholders cannot be reimbursed by a liability policy that names the litigant as a policyholder; although this risk can be mitigated in some circumstances with a ‘cross-liability’ clause.

Unless the relationship between authority and the supplier is not carefully and formally documented there can be unexpected questions as to who is the employer of the workforce. It is not just about who pays wages; but the legal relationship may be confused when detailed directions and control is by another party. If a person is deemed in law to be an employee, there is of course a statutory responsibility to have employer’s liability insurance.

Suppliers’ extensions are again possible to arrange but these will be with inner limits and cover restrictions. Needless to say, great care is needed in construction of the insurance portfolio to avoid unpleasant surprises; not least where new risks are being presented.

Conventional insurance programmes provide, of course, massive value, though they are, by nature financial management tools. They do not set out to protect the insured against non-financial loss or damage.

Uninsured or even uninsurable damage can include available workforce skills, the ability to communicate, reputation failure and service users’ reaction to that failure, legal and operational access to crucial information, legality, compliance, and security. There is a core need also to remain in control, financially and operationally, and to be able to respond fast enough to an incident to meet urgent responsibilities. These additional risks are matters for risk management, not insurance.

The opportunities will emerge from the embedding of risk concerns into all the processes. This is further described in Appendix 1 – Embedding risk control procedures.

**Myth 9: We don’t need risk management, we have insurance**

This is a subject that could justify a paper in itself but we must restrict ourselves here to headlines only and stay within the context of outsourcing.

The key message is that there are real dangers in simply assuming that conventional insurance policies will transfer seamlessly when the cause of that stress is damage to the outsourcing contractor.

Simply making the counterparty a joint insured has its dangers too, not least because if that counterparty fails to meet any of the policy requirements or fails to disclose material facts, then the entire policy is void. Furthermore, any claims for failure between the two policyholders cannot be reimbursed by a liability policy that names the litigant as a policyholder; although this risk can be mitigated in some circumstances with a ‘cross-liability’ clause.

Unless the relationship between authority and the supplier is not carefully and formally documented there can be unexpected questions as to who is the employer of the workforce. It is not just about who pays wages; but the legal relationship may be confused when detailed directions and control is by another party. If a person is deemed in law to be an employee, there is of course a statutory responsibility to have employer’s liability insurance.

Care is needed also with material damage covers. Conventional material damage cover provides protection against named perils; and even where there is a ‘suppliers’ extension’, the original cause of the loss may still need to be one of the named perils. The minefields are just the same with business interruption covers which are adjunct to material damage covers with all their values and limitations.
5. The civil society – its opportunities and additional challenges

5.1 Working with the civil society

Contracting with the Third Sector or civil society, more specifically charities, social enterprises and local community (voluntary) groups, to deliver services and responsibilities is, conceptually, no different from contracting with other organisations. The process, as always, begins with ensuring that there is a clear recognition of the responsibilities that are being passed over, and above all the extent of the damage that would be caused should the supplier fail the authority.

It is when we now begin to move forward that some of the quite special challenges of the civil society need to be considered. Politically, there is an urge to use civil society organisations and there are numerous papers where authorities are encouraged to give additional support to tenders by charities, social enterprises and local community groups. This encouragement, however, is mostly to reduce the challenges, resources and paperwork. This, however, reduces the information and controls that an authority would normally wish to have for risk assessments. This section of the paper brings out the additional aspects of dealing with the civil society and, by the use of effective and constructive risk management, ensures, in the face of these aspects, that all parties can go forward comfortable within the relationships created.

An authority may have a wish to remain local, and to use a particular charity if that charity has already been delivering much-needed and related values into the community for some years. The charity has probably been encouraged in the past by grants from Government funds as well as other fundraising. The Sustainable Community Strategy may though turn this ‘nice to have’ charity service delivery into one of the authority’s own strategic objectives. There is a clear logic, if the charity has been performing well, to encourage that charity to continue in a contracted role. Indeed, to move the task away from a charity to a company or other organisation is very likely to cause community discomfort.

An authority may be encouraged to shorten the bidding and decision-making processes to assist a low resourced charity to get the job, but the authority is left with the normal risks of outsourcing and, additionally, the special risks of partnering with civil society organisations. These risks should not be put to one side in the urge to shortlist them.

The risks remain and have some unique dimensions to be managed; whether it be the authority’s risk of failure; or risks to both parties if the authority has encouraged a civil society organisation to take a contract that it is not fully able to deliver. Furthermore, one or both of the parties may have not understood the fundamental change in legal and other liabilities when a charity’s mission becomes a contracted responsibility.

The statement below goes so far as to acknowledge that authorities perceive some barriers in working with Third Sector (or civil society) suppliers.

However, the Funding and Procurement Compact Code of Good Practice COI 2008 addresses the need for early understanding of exposures:

4.7 The Government undertakes to explain and agree terms of delivery (such as success and performance criteria) with the voluntary and community organisation before the contract or funding agreement is entered into. This should include the actions that will be taken if the voluntary and community organisation is failing to deliver. Departments and Agencies should be sensitive to the impact which changes in the contract can have. They should ensure that there is a simple and pre-agreed process for controlling change and that account is taken of comments from the voluntary and community organisation on the changes required.

4.8 The Government undertakes to discuss risks up-front and place responsibility with the public sector body or voluntary and community organisation best able to manage them. In particular, Government should consider and address the risks associated with the demand for a particular service.”
5.2 Unique risks of dealing with civil society organisations

There are unique risks when dealing with the civil society that will need to be embraced alongside the other routine risk work and scenario setting. In headline form, they can be listed as below.

- **Moving from a mission to a contracted responsibility**
  - charities and other similar organisations often work to deliver on their own wish list and what they feel they can deliver from the resources available to them. A business approach conversely begins with a careful and prioritised measurement of the community-wide needs and priorities, then responding to them.
  - this is a fundamental shift in the balancing act of responsibility and the resources available to meet the responsibility.

- **Adequacy of Resources**
  - local charities especially, are rarely large enough to have sufficiently skilled resources that will enable them to devote the necessary time and energies to understanding their risks and then professionally managing them.
  - this includes meeting the authority's own control standards.
  - the change to contracted relationship will mean that all parties will need to understand their new risks. This may demand risk understanding and management skills previously felt not to be needed.

- **Financial resilience**
  - their financial resilience may be seriously exposed to insecure sources of funding, such as grant decisions made year by year.
  - they may be inadequately reserved to face unexpected financial hits, and just as in business, may face unexpected new charges. An example is likely to be the new Pension Fund requirements of 2012.
  - there are ways that a charity may lose its charity status. Such loss could destroy the financial models on which they depend.

- **Consortia bidding and relationships**
  - charities may need to tender within a consortium to be able to deliver towards the required services.
  - there are both outsourcing and partnership working exposures with interdependencies that will need to be understood not only by the consortium leader but by the authority as well.

- **Other tasks and wish lists**
  - the charity may wish to continue to deliver on wish lists that are beyond the authority’s contracted services.
  - the charity may be dependent on traditional grants and fundraising to deliver these other tasks. Failure to achieve these fundraising targets could put the entire charity at risk of failure; and thus include the specific tasks that have been more formally contracted.

- **Trusted succession**
  - much more than in companies, charities can be inspirationally dependent on one dominant trustee, worker or a small team of workers. They may not have adequate succession planning.

- **Trustee skills**
  - smaller charities will often recruit their trustees from people who are willing to volunteer their time, rather than a considered approach that first identifies the balance of skills needed, then importing those particular skills.

- **Recourse for damage**
  - the authority normally may be able to take legal steps to demand compensation from suppliers that fail them. Taking a charity to court, however, and perhaps threatening its future existence is emotionally a much more difficult decision and one certainly that could attract adverse media and community reaction.
  - not least, this would damage the authority’s own confidence.

- **Work style and vision**
  - a charity may find it culturally difficult to change its work style and deliver on a contract that has in turn been driven by the authority’s Local Area Agreement (LAA) targets.
  - this may need them to recognise that the role has now moved to one measured against a contracted public service strategic objective; and not just a reactive one driven by the charity trustees’ own feelings and wishes.

We need also to consider the charity’s own pressures:

> “to succeed, a charity must remain true to its aims and vision. if donors and volunteers sense that it is moving away from its original purpose their support will diminish. if a charity that delivers public services begins to be perceived as another arm of government, donors may feel that they are taking up a burden that should be borne by taxpayers and volunteers may feel that they are simply becoming used as substitutes for public servants.”

**Perception and Reality. the real risks for public service and charitable organisations. Zurich 2007.**

5.3 Additional demands on the authority’s resources

Charities, social enterprises and community voluntary groups may need guidance on how they can, more professionally, and in a measured way, ensure that they deliver on those new objectives. The charity, supported by grants from well-wishers, will almost certainly find that the contract has changed its legal status. It has assumed new legal responsibilities under contract, and may now be subject to charges of nonfeasance as well as malfeasance; not to mention a range of new responsibilities under statute. Thus, moving a relationship from grandparents to contractual changes the litigation risks. This may demand risk understanding and management skills previously felt not to be needed.

These preferences and constraints will need to be respected and yet, delicately, not be allowed to get in the way of the contracted responsibilities. Getting the charity to change its mindset and respond to an entirely new role may be a challenge that is not straightforward.

It is a fine and difficult balancing act between:

a) Setting demands on the charity to prove its resilience
b) Demanding activity that is proportionate to the ability of that charity to meet those demands
c) Retaining only acceptable exposures for the authority in meeting its own responsibilities
d) Building into the budgeting the cost of ongoing resources that may be needed to support the charity and keep it within the authority’s risk tolerance profile and

- the above could include additional support in business continuity planning, back up of data, insurance, legal advice, trustee support, and other routine risk tasks.
A New World of Risk

6. Exit strategy

6.1 The importance of an agreed exit strategy

Throughout this paper we have stressed that all outsourcing relationships must have an exit strategy.

The reality is that enthusiastic project managers and sponsors do not always accept that their branchchild could go wrong or at least may need to evolve to respond to change. We have quoted survey results showing just how many outsourcing arrangements have had to be closed or changed. One, A Diamond Cluster International Survey reported that 78% of responding executives had had to terminate agreements early due to poor service, a change in a strategic direction, or costs (Source: DiamondCluster International, 2002).

The problem with the supplier could be a sudden accidental failure, insolvency, or a gradually evolving problem. A supplier who has an emerging quality problem that is beginning to affect stakeholder trust in the authority is no less destructive. It raises difficult questions of when to intervene, balancing a need to embrace the delivery responsibilities of the partner organisation.

It must position the authority so that it has access to all it needs to take back the activity or be able to transfer it to another third party whilst at the same time continuing to maintain urgent and essential services. As always, the need and complexity of such a pre-nuptial agreement will depend on the level of risk, the perceived potential for damage; and the speed by which replacement services need to be introduced.

The cost of retaining relationships with duplicate suppliers, or maintaining reserve stock levels, may not please the accountant minded, but those extra costs may be considered by the strategist to be cost-effective risk management expenditure; and be a part of the exit strategy. Having duplicated sources of supply will also mean that, if anything important has been passed over, it has been passed to more than one point of risk.

Dealing with the third sector or civil society does bring its own challenges but effective risk management not only manages these risks but can be an enabler where this is the preferred policy.
The exit agreement, sometimes known as transition management or transition continuity agreement, will cover how the notice to exit is delivered, and the timing and format of the termination. It will deal with records, data, and reports. The ultimate risk is an organisational divorce; and this will need, even more, to have an agreed record of the various dependencies that may have been passed over to the supplier.

The legal and physical transfer of hardware, buildings and their contents needs to be pre-agreed, and with agreement of the method by which such assets will be valued. The market value, even if there is one, is unlikely to be the only consideration to one party who now needs them so much more urgently than the other.

Ownership and use of an electronic database of personal client information may require pre-registration as custodians and purpose of use within the Data Protection Act UK 1998 (or similar). Information is not just constrained to that which is on electronic databases. There is a whole range of other intellectual assets that may have formed part of the relationship; not least patents, copyrights, trademarks, brand names, domain names, websites, email addresses and their exclusivity. There can be research materials and the implied right to use that material. The ownership of outstanding liability claims to or from third parties and between themselves or those whom the insurances will now protect may not otherwise be clear.

The process of divorce brings service delivery problems, but can also bring many legal issues, compliance, brand, human problems and questions around ownership of both physical and intellectual property. Engineering a structured and calm separation enables the core dependencies to be recovered, managed and used throughout the divorce process without damage.

Ownership of outstanding liability claims to or from third parties and between themselves or those whom the insurances will now protect may not otherwise be clear.

The detailed schedule of activities and legalities can also include the agreement on ownership and access to intellectual assets, work in progress and how assets can remain in secure, good, accessible and usable order. This may not be as straightforward as it sounds. The transfer of technology hardware, software or data may need to include the skills and manuals to maintain these tools and any software codes that will enable technicians to do so.

Separation may take weeks or months. The transfer agreement can usefully embrace therefore, the responsibilities and activities of each party and the reimbursement of costs and lost revenues whilst that separation is under way. Any process of subsequent re-engineering will need its own change management and control processes to be followed through.

Ownership and use of an electronic database of personal client information may require pre-registration as custodians and purpose of use within the Data Protection Act UK 1998 (or similar). Information is not just constrained to that which is on electronic databases. There is a whole range of other intellectual assets that may have formed part of the relationship; not least patents, copyrights, trademarks, brand names, domain names, websites, email addresses and their exclusivity. There can be research materials and the implied right to use that material. The ownership of outstanding liability claims to or from third parties and between themselves or those whom the insurances will now protect may not otherwise be clear.

The future position of employees will need to be agreed beforehand, including the responsibility for redundancy payments and pensions. Ensuring continuing employee motivation is also a communications challenge; recognising that both organisations may not at the time have the same incentive to do so. Audit and compliance trails are vital dependencies and announcements to service users, auditors, and other stakeholders are best engineered beforehand in a spirit of co-operation and (hopefully) a mutual protection of reputations.

Ownership and use of an electronic database of personal client information may require pre-registration as custodians and purpose of use within the Data Protection Act UK 1998 (or similar). Information is not just constrained to that which is on electronic databases. There is a whole range of other intellectual assets that may have formed part of the relationship; not least patents, copyrights, trademarks, brand names, domain names, websites, email addresses and their exclusivity. There can be research materials and the implied right to use that material. The ownership of outstanding liability claims to or from third parties and between themselves or those whom the insurances will now protect may not otherwise be clear.

The legal and physical transfer of hardware, buildings and their contents needs to be pre-agreed, and with agreement of the method by which such assets will be valued. The market value, even if there is one, is unlikely to be the only consideration to one party who now needs them so much more urgently than the other.

Ownership and use of an electronic database of personal client information may require pre-registration as custodians and purpose of use within the Data Protection Act UK 1998 (or similar). Information is not just constrained to that which is on electronic databases. There is a whole range of other intellectual assets that may have formed part of the relationship; not least patents, copyrights, trademarks, brand names, domain names, websites, email addresses and their exclusivity. There can be research materials and the implied right to use that material. The ownership of outstanding liability claims to or from third parties and between themselves or those whom the insurances will now protect may not otherwise be clear.

The detailed schedule of activities and legalities can also include the agreement on ownership and access to intellectual assets, work in progress and how assets can remain in secure, good, accessible and usable order. This may not be as straightforward as it sounds. The transfer of technology hardware, software or data may need to include the skills and manuals to maintain these tools and any software codes that will enable technicians to do so.

Separation may take weeks or months. The transfer agreement can usefully embrace therefore, the responsibilities and activities of each party and the reimbursement of costs and lost revenues whilst that separation is under way. Any process of subsequent re-engineering will need its own change management and control processes to be followed through.

Ownership and use of an electronic database of personal client information may require pre-registration as custodians and purpose of use within the Data Protection Act UK 1998 (or similar). Information is not just constrained to that which is on electronic databases. There is a whole range of other intellectual assets that may have formed part of the relationship; not least patents, copyrights, trademarks, brand names, domain names, websites, email addresses and their exclusivity. There can be research materials and the implied right to use that material. The ownership of outstanding liability claims to or from third parties and between themselves or those whom the insurances will now protect may not otherwise be clear.

Ownership and use of an electronic database of personal client information may require pre-registration as custodians and purpose of use within the Data Protection Act UK 1998 (or similar). Information is not just constrained to that which is on electronic databases. There is a whole range of other intellectual assets that may have formed part of the relationship; not least patents, copyrights, trademarks, brand names, domain names, websites, email addresses and their exclusivity. There can be research materials and the implied right to use that material. The ownership of outstanding liability claims to or from third parties and between themselves or those whom the insurances will now protect may not otherwise be clear.

The reality of course is that, however carefully a contract is worded, it does not mean that the contract clauses will lead to a calm and mutually supportive exit. This is especially so if the separation is hostile or caused by the operational or financial failure of one of the parties. That reality also may be that one of the parties simply will be unable to proceed to exit as hoped. Appointed liquidators will set out to secure anything of value to meet their own legal responsibilities to gain maximum financial value for the benefit of their own, failed principle’s creditors. It can be immensely valuable, however (especially in the short term) if the counterparty that has been let down knows they still have the legal and operational ability to gain possession and use of these critical dependencies. This right of access under contract may at least avoid a liquidator putting an inflated value on them at the time of separation because of the authority’s desperation.

The exposure that the counterparty will not perform as contracted within the exit clauses is equally a risk management issue and that possible failure needs also to be thought through beforehand. The best answer is that the relationship is created so that there will always be a balance of incentives for each party to support the other. This may not be possible of course and plan B is always to ensure the ability to meet critical and urgent responsibilities is retained or duplicated at all times; both in law and from an operability point of view. Some answers may be straightforward and others may be much more difficult and expensive to implement but, if the risk and potential impact is important enough, the authority may need to invest in the wherewithal to be able still to deliver itself or through other partners.
7. Governance and benchmarking

7.1 Existing control and governance

There is a very wide range of standards and benchmarking opportunities, and we can here cover just a few of them. The CIPFA document, Delivering Good Governance in Local Government 2007 provides a valuable definition of governance and introduction to this section.

The Audit Commission states on its website that ‘Key lines of enquiry (KLOE) are detailed questions that help to inform our inspection judgements’. They are used by Audit Commission inspection teams and also published in order to help audited and inspected bodies with their own assessments. KLOE audit requirements demand and will measure risk issues that include outsourced dependencies; specifically:

KLOE 2.3

Does the organisation promote and demonstrate the principles and values of good governance?

KLOE focus: The organisation:

• Has adopted, promotes and demonstrates, the principles of good governance
• Maintains focus on its purpose and vision
• Demonstrates a strong ethical framework and culture; and
• Applies the principles and values of good governance to its partnership working

KLOE 2.4

Does the organisation manage its risks and maintain a sound system of internal control?

KLOE focus: The organisation:

• Has effective risk management which covers partnership working
• Has a clear strategy and effective arrangements, including allocation of appropriate resources, to manage the risk of fraud and corruption; and
• Has a sound system of internal control including internal audit

There is a wide range of documents that reinforce these messages, one of which is as below:

The document ‘Effective Partnering’ (OGC, 2003) talks of the positioning of a ‘Senior Responsible Owner’ in the customer organisation and a Senior Responsible Industry Executive within the provider organisation. We call the role a ‘Risk Tsar’ (see Appendix 1 – Embedding risk control procedures). It also talks of a shared risk register and a joint project board.

...putting in place the following key elements:

• an annual risk assessment which identifies the key risks to outcomes or delivery for each area
• an annual scored Use of Resources judgement for local public sector bodies, drawn from the annual audit
• an annual scored Direction of Travel judgement which assesses the effectiveness of each local authority in driving continuous improvement
• inspection activity by relevant inspectorates targeted primarily on the basis of the risk assessment


An over focus on satisfying regulatory requirements can however be a huge danger if those requirements supersede the effective strategic management of the responsibility. Replacing good management with regulatory satisfaction is not good management but if clear vision is maintained, it can be mutually inclusive.

This will include all audit, benchmarking, outcome measurement, risk communication models, project outcomes, and stress testing that are already embedded. Integrating them across different organisations is a task in itself.

It may entail the integration of management systems between the authority and the outsourcing company. One benchmark that may systems between the authority and the outsourcing company. One benchmark that may be useful is the Collaborative Business Relationships. Published Standards

There are tools that will enable an organisation to take a helicopter view on the resilience of themselves and the resilience of others. A common one within the United Kingdom is British Standard BS25999 – Business Continuity Management – and there is also a risk standard – BS31100 – Code of Practice for Risk Management.

The BS25999 Standard establishes a six-step process cycle described as below:

1. BCM programme management

• Programme management enables the business continuity capability to be both established (if necessary) and maintained in a manner appropriate to the size and complexity of the organisation

2. Understanding the organisation

• The activities associated with ‘Understanding the organisation’ provide information that enables prioritisation of an organisation’s products and services at an acceptable level of operation; and, within an acceptable timeframe during and following a disruption

3. Determining business continuity strategies

• Determining business continuity strategies enables a range of strategies to be evaluated. This allows an appropriate response to be chosen for each product or service, such that the organisation can continue to deliver those products and services at an acceptable level of operation; and, within an acceptable timeframe during and following a disruption
A New World of Risk

4. Developing and implementing a BCM response

- Developing and implementing a BCM response results in the creation of a management framework and a structure of incident management, business continuity and business recovery plans that detail the steps to be taken during and after an incident.

5. BCM exercising, maintaining and reviewing BCM arrangements

- Exercising, maintenance, review and audit lead to the organisation being able to demonstrate the extent to which its strategies and plans are complete, current and accurate; and identify opportunities for improvement.

6. Embedding BCM in the organisation’s culture

- Embedding BCM in the organisation’s culture enables BCM to become part of the organisation’s core values and instills confidence in all stakeholders in the ability of the organisation to cope with disruptions.

(www.bsi-global.com)

This Standard has many values, but is also a false dawn when dealing with the fallout from a third party’s failure. It is, sadly, just too easy to ask the potential supplier to tick a box that they are ‘25999 compliant’. Compliance with the standard will indeed give that organisation a better than average chance of surviving a threatening incident itself as, to be compliant, it has illustrated that it has taken a careful look at its own sensitivities and survival needs, protected them, and produced a survival plan. What the supplier’s compliance does not guarantee is that the 25999 resilient organisation will continue to deliver products or services to each and every one of its customers according to the customers’ (or the authority’s) own sensitivities and urgencies. Many a continuity plan will prioritise its customers, according to their perceived importance to the supplier. The receiving authority’s own vital dependencies and sensitivities will be very different from those of the supplier, and may be sacrificed by a supplier fighting for its own survival.

With outsourced dependencies, satisfying BS25999 therefore is only a starter for a discussion that moves on to negotiations about the sensitivities and urgencies of the authority too and the gaining of trusted assurances that those sensitivities are part of the continuity work of the supplier.

A supplier’s compliance with BS25999 will mean that there is an exercised recovery plan. There is no demand within the standard that that recovery plan will fit comfortably alongside each of its customer’s own plans. It is possible that a service delivery failure will place both organisations into crisis and demand the triggering of each of their recovery plans. If these plans do not communicate, nor work to common objectives and targets, chaos can too easily result.

The ‘Orange Book’ (The Orange Book: Management of Risk – Principles and Concepts. HM Treasury) is a general risk management standard and refers to a Risk Management Assessment Framework that asks for a statement on internal controls. The Audit Commission has of course produced a wide range of papers and guides, notably the Delivery Chain Analysis – removing obstacles to local joint working (Working Better Together, 2009).

Appendix 1: Embedding risk control procedures

Consistent controls across the management team and staff of a large and diverse organisation will never occur by accident.

1. Could have an impact or change any group brand and reputation
2. Will need changes in group wide arrangements and services such as the governance, insurance, continuity, health and safety programmes
3. Enters a new country or territory
4. Delivers a new product or service
5. Could impact the market, workforce or product of another division
6. Could affect the legal or regulatory requirements on the group
7. Could affect the confidence of employees and other stakeholders
8. Is likely to attract significant or negative media interest
9. Significantly changes the financial gearing of the division
10. Any that could change the risk profile of the group
Any significant proposal should always require a statement of risk issues, changes in risk profiles and how they are to be handled, yet significance needs to be measured against the wider impact not by the amount of money spent.

No contract should be signed with any third party for supply or delivery of goods or services without a documented statement of risk and continuity risks involved and how these risks are factored and priced into the relationship. Other soft and hard controls to reduce the risk of surprise may include the following checklist:

- The direct reporting structure of risk professionals needs to be at a level that will ensure an audience at the most senior level of decision making
- The training, background and experience of risk professionals must be such that they will earn confidence when discussing board level business models and strategies
- Awareness that measured, informed and consistent risk tolerance is part of the risk professional’s task
- Routine reporting and presentations on risk issues be required directly to audit committee, risk committee or equivalent

- **A Risk Tsar** operating at the organisation’s highest strategic decision-making level to empower and prioritise risk issues across the whole organisation. A key task of the risk tsar is to ensure risk remains always on the agendas and in decision making. Further risk tsars may be valuable at subsidiary or key business unit levels where high levels of risk are perceived; with direct communication to the supplier’s equivalent
- Risk awareness and sensitivity measures need to be set into employees’ all generic Key Task Objectives set by the human resources department. This should embrace medium and longer-term risks within any shorter-term performance measurement and bonus systems and thus become part of performance assessments
- Management information tools and the reporting of the performance of business units are mandated to be risk-measured
- Make full use of non-executive directors for risk issues
- Co-operation, communication and use of all fellow risk professionals across the organisation, their tools, powers and influence
- Embedding risk into the organisation’s vision and policy statements; with an individual risk policy statement in support
- Framework requirements for board papers, project and other proposals and objectives should be mandated to embrace a chapter paragraph on any risks within the project; and also the potential impact on financial and non-financial risks of the rest of the organisation
- Budgeting for risk management activity is not a matter for the risk professional; nor is the taking of decisions around which risks are or are not acceptable

The role of the risk professional is to inform and advise the chief executive, operational manager or board in matters of risk and potential consequence.

If a measured risk is considered by the operational manager to be unacceptable, the problem remains with the operational manager. If the risk is significant, the do-nothing option is not available to that manager. He or she must, often by law or corporate governance requirements, do something about it; not least communicate it to stakeholders. The risk manager can further add value by advising on risk and consequence management options and the cost of such options. It is then for the operational manager to decide and budget within the unit’s own finances.

- The risk professional can add real cost effectiveness values by bringing together different units’ risk needs within a common risk management investment; and then debiting that cost proportionately back into the units’ own finances. This retains ownership, visibility and cost/benefit analyses within those units
- Often the best way of encouraging risk awareness is to demand that the consequence of risk be retained within each operational unit’s performance figures. This is of value when the consequences of the risk are not potentially catastrophic to the parent organisation. For example, the reduction of group motor insurance to third party only will mean that damage will be debited to the unit and attract the unit manager’s interest in the quality of individual driving standards; driver profiles, driver reward systems etc
Appendix 2: Suggestions for contract headings

In practice contracts will embrace many needs of their own but this list may be useful as a generic starting point for project designers.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Definitions and interpretation</td>
</tr>
<tr>
<td>2.</td>
<td>Grant of licences</td>
</tr>
<tr>
<td>3.</td>
<td>Product or service to be delivered</td>
</tr>
<tr>
<td>4.</td>
<td>Minimum service levels in the face of disruption to normal working</td>
</tr>
<tr>
<td>5.</td>
<td>Indemnities and their measurement of value</td>
</tr>
<tr>
<td>6.</td>
<td>Liabilities adopted and to be protected</td>
</tr>
<tr>
<td>7.</td>
<td>Quality, controls and right of access</td>
</tr>
<tr>
<td>8.</td>
<td>Pricing of orders and forecasts</td>
</tr>
<tr>
<td>9.</td>
<td>Packaging and packaging materials</td>
</tr>
<tr>
<td>10.</td>
<td>Disputes and their resolution</td>
</tr>
<tr>
<td>11.</td>
<td>Communications and notice of potential disruption</td>
</tr>
<tr>
<td>12.</td>
<td>Relationship management and agreed procedures</td>
</tr>
<tr>
<td>13.</td>
<td>The contractor’s constraints and responsibilities</td>
</tr>
<tr>
<td>14.</td>
<td>The principal’s constraints and obligations</td>
</tr>
<tr>
<td>15.</td>
<td>Resilience management and the interface between continuity plans</td>
</tr>
<tr>
<td>16.</td>
<td>Titles</td>
</tr>
<tr>
<td>17.</td>
<td>Risk profiles, change management and right to access and audit</td>
</tr>
<tr>
<td>18.</td>
<td>Storage</td>
</tr>
<tr>
<td>19.</td>
<td>Indemnity and insurance</td>
</tr>
<tr>
<td>20.</td>
<td>Pricing methodology</td>
</tr>
<tr>
<td>21.</td>
<td>Payments and payment schedules</td>
</tr>
<tr>
<td>22.</td>
<td>Intellectual property ownership and protection</td>
</tr>
<tr>
<td>23.</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>24.</td>
<td>Term and exit agreement</td>
</tr>
<tr>
<td></td>
<td>• Consequences of termination</td>
</tr>
<tr>
<td></td>
<td>• Force majeure</td>
</tr>
<tr>
<td></td>
<td>• Assignment</td>
</tr>
<tr>
<td></td>
<td>• Knowledge transfer, including continuing technical advice and support</td>
</tr>
<tr>
<td></td>
<td>• Facilitation of supplier change</td>
</tr>
<tr>
<td></td>
<td>• Information and other security</td>
</tr>
<tr>
<td></td>
<td>• Rights and duties during the process of remuneration, individual and cumulative</td>
</tr>
<tr>
<td></td>
<td>• Costs and cost controls</td>
</tr>
<tr>
<td></td>
<td>• Removal of supplier property and/or return of principal’s property</td>
</tr>
<tr>
<td></td>
<td>• Records and data transfer</td>
</tr>
<tr>
<td></td>
<td>• Interim services and</td>
</tr>
<tr>
<td></td>
<td>• Supplier responsibilities</td>
</tr>
<tr>
<td></td>
<td>• Principal responsibilities</td>
</tr>
<tr>
<td></td>
<td>• Exit plan, exercising and version control</td>
</tr>
<tr>
<td>25.</td>
<td>Invalidity</td>
</tr>
<tr>
<td>26.</td>
<td>Product or service recall; leadership and responsibilities</td>
</tr>
<tr>
<td>27.</td>
<td>Notices</td>
</tr>
<tr>
<td>28.</td>
<td>Relationships of the parties</td>
</tr>
<tr>
<td>29.</td>
<td>Set off</td>
</tr>
<tr>
<td>30.</td>
<td>Laws and jurisdiction</td>
</tr>
</tbody>
</table>
Appendix 3: Benchmarking and Standards

In practice contracts will embrace many needs of their own but this list may be useful as a generic starting point for project designers.

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
</table>
| Delivering Good Governance in Local Government. (CIPFA 2007) | The document requires the authority to:  
  - Consider the extent to which the authority complies with the principles and requirements of good governance set out in the Framework  
  - Identify systems, processes and documentation that provide evidence of compliance  
  - Identify the individuals and committees responsible for monitoring and reviewing the systems, processes and documentation identified  
  - Identify the issues that have not been addressed adequately in the authority and consider how they should be addressed  
  - Identify the individuals who would be responsible for undertaking the actions required and plan accordingly  
In the context of partners and outsourcing:  
  - Members should be clear about their roles and responsibilities both individually and collectively in relation to the partnership and to the authority when working in partnership  
  - Ensure there is clarity about the legal status of the partnership  
  - Ensure representatives of organisations both understand and make clear to all other partners the extent of their authority to bind their organisation to partner decisions |
| Business Case Self Assessment and Auditor’s Checklist | Developed in 2007 by The Improvement and Development (IdeA), Communities and Local Government (CLG) and the London Borough of Lambeth the document provides valuable self-assessed checklists. Whilst there is no specific reference to outsourcing or partnering, the principles outlined embrace the outsourcing challenges. |
| BS ISO/IEC 27001:2005 | Information technology. Security techniques. Information security and management systems. This is a standard to cover all types of organisations from commercial enterprises, government agencies to non-profit organisations. This international standard will provide a specification for ISMS within the context of the organisation’s overall business risks and the foundation for third party audit and certification. |
| BS ISO/IEC 16085:2006 Systems and software engineering. Life cycle processes. Risk management | BS ISO/IEC 16085:2006 describes a process for the management of risk during systems or software acquisition, supply, development, operations, and maintenance. The purpose of this standard is to provide suppliers, acquirers, developers, and managers with a single set of process requirements suitable for the management of a broad variety of risks. |
| BS25999 Business Continuity Management | This is the 2006 standard on business continuity management and part two sets out the steps that can lead to certification under this standard. The requirements are embraced in the chapter on business continuity. Part 2 (2007) established the requirement for independent certification. |
| PAS 11000 Collaborative Business Relationships | Prompts and sets standards for collaboration between organisations. |
| PAS 99:2006 Specification of common management system requirements | A framework for integration management, suitable for any organisation, regardless of size or sector, looking to integrate two or more of their management systems into one cohesive system with a holistic set of documentation, policies, procedures and processes. |
| ISO/PAS 28000:2005 Specification for security management systems for the supply chain | This Publicly Available Specification (PAS) has an objective to improve the security of supply chains. It supports an organisation’s work to establish an overall supply chain security management system. It requires the organisation to assess the security environment in which it operates and to determine if adequate security measures are in place. |
Appendix 4: The 12 Strategic Questions, Audit Commission

This has been reproduced from the Audit Commission white paper: Working better together – delivery chain analysis (2009).

This self-assessment helps LSPs to develop delivery chains and plan the delivery of LAA outcomes. It may be used separately for each outcome or applied to delivery planning for the whole agreement.

Please score each question separately as red, amber, or green. Red responses should be scored -1, amber 0, and green +1. Scores of between 9 and 12 suggest an effective and efficient delivery plan. Between 3 and 8 suggests risks to delivery and reduced efficiency. Scores of less than 2 point out that significant improvement is needed. Scores between -3 and -8 suggest inefficiency and ineffective delivery and -9 to -12 shows a high degree of failure.

Where responses are shown as red then action is required urgently to facilitate planning.

### 1. Is the outcome clearly defined?

<table>
<thead>
<tr>
<th>RED</th>
<th>-1</th>
<th>The outcome is vague and its measurement is complex.</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMBER</td>
<td>0</td>
<td>The outcome is clear but not all partners are signed up and measurement is difficult.</td>
</tr>
<tr>
<td>GREEN</td>
<td>+1</td>
<td>The outcome is clearly defined, understood and agreed by partners.</td>
</tr>
</tbody>
</table>

### 2. Is the evidence base sufficiently robust?

<table>
<thead>
<tr>
<th>RED</th>
<th>-1</th>
<th>Little research and no piloting resulting in a weak evidence base.</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMBER</td>
<td>0</td>
<td>Some research on existing evidence highlights factors on which to focus but this is not implemented at all levels resulting in a high failure risk.</td>
</tr>
<tr>
<td>GREEN</td>
<td>+1</td>
<td>Extensive preliminary research and piloting of interventions. Interventions at all levels and across agencies are aligned maximising effectiveness and minimising cost.</td>
</tr>
</tbody>
</table>

### 3. Is there sufficient capacity, including available resources, to deliver?

<table>
<thead>
<tr>
<th>RED</th>
<th>-1</th>
<th>No resource assessment across the delivery chain resulting in a risk of misdirecting resources.</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMBER</td>
<td>0</td>
<td>Assessment of resource availability is undertaken and capacity issues are being addressed.</td>
</tr>
<tr>
<td>GREEN</td>
<td>+1</td>
<td>Keen awareness of resource and capacity issues. Resource is directed to where it is most effective and capacity is regularly reviewed.</td>
</tr>
</tbody>
</table>

### 4. Is there a shared partnership operational plan describing how services/interventions will be provided?

<table>
<thead>
<tr>
<th>RED</th>
<th>-1</th>
<th>No cohesive cross-agency operational plan. Some individual partner documents.</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMBER</td>
<td>0</td>
<td>An operational plan exists but most delivery partners have not been involved in its production nor is it widely available.</td>
</tr>
<tr>
<td>GREEN</td>
<td>+1</td>
<td>An operational plan exists, produced with all delivery partners; widely available and well understood. Front line staff and service users consulted.</td>
</tr>
</tbody>
</table>

### 5. Are the objectives supported by a funding strategy?

<table>
<thead>
<tr>
<th>RED</th>
<th>-1</th>
<th>Funding identified or multiple short-term funding streams with funding not dependent on performance.</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMBER</td>
<td>0</td>
<td>Longer-term funding allows more certainty, but there are still multiple overlapping streams. Some performance-related funding.</td>
</tr>
<tr>
<td>GREEN</td>
<td>+1</td>
<td>Funding streams mapped as part of strategy development; number of funding streams rationalised. Funding is structured to incentivise performance and awarded on proven performance. Where appropriate, funding periods are extended.</td>
</tr>
</tbody>
</table>

SCORE
6. Do the various partners and levels within them communicate regularly using reliable information so that there is good coordination?

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RED</strong></td>
<td>-1</td>
<td>No mechanism in place for the different partners and levels of the delivery chain to come together and address issues.</td>
</tr>
<tr>
<td><strong>AMBER</strong></td>
<td>0</td>
<td>Some coordination but insufficient to create a common understanding of risks and issues facing delivery.</td>
</tr>
<tr>
<td><strong>GREEN</strong></td>
<td>+1</td>
<td>Regular contact between all levels of the delivery chain. Active communication between the front line and the centre so that front line information informs strategic decision making across partners.</td>
</tr>
</tbody>
</table>

**SCORE**

7. Are levers and incentives fit for purpose?

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RED</strong></td>
<td>-1</td>
<td>Few levers or incentives in place.</td>
</tr>
<tr>
<td><strong>AMBER</strong></td>
<td>0</td>
<td>Some incentives in place. Levers are established but without consultation; not piloted so not always the effective ones.</td>
</tr>
<tr>
<td><strong>GREEN</strong></td>
<td>+1</td>
<td>Incentives are fit for purpose. Levers are based on context and the ability of individual partners to respond.</td>
</tr>
</tbody>
</table>

**SCORE**

8. Are the risks to the delivery chain well managed?

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RED</strong></td>
<td>-1</td>
<td>No risk assessment is undertaken.</td>
</tr>
<tr>
<td><strong>AMBER</strong></td>
<td>0</td>
<td>Internal partner risk assessment is undertaken; but awareness of key risks is not cascaded through the delivery chain.</td>
</tr>
<tr>
<td><strong>GREEN</strong></td>
<td>+1</td>
<td>Thorough partnership risk assessment is undertaken; risk management culture exists throughout the delivery chain. Each stage of the chain has a high awareness of key risks.</td>
</tr>
</tbody>
</table>

**SCORE**

9. Do performance management systems enable tracking of delivery?

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RED</strong></td>
<td>-1</td>
<td>Multiple performance management systems; hard to measure.</td>
</tr>
<tr>
<td><strong>AMBER</strong></td>
<td>0</td>
<td>Performance management systems can measure progress but indicators are not entirely accurate or have other weaknesses.</td>
</tr>
<tr>
<td><strong>GREEN</strong></td>
<td>+1</td>
<td>Shared systems in place. Regular monitoring. Frequent stock takes. Performance easy to track against objectives. Routine corrective action.</td>
</tr>
</tbody>
</table>

**SCORE**

10. Is there strong leadership that is accountable through clear governance structures at all levels of the delivery chain?

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RED</strong></td>
<td>-1</td>
<td>Leadership is poorly assigned. Shortage of clear guidance results in lack of clarity about who should take the lead.</td>
</tr>
<tr>
<td><strong>AMBER</strong></td>
<td>0</td>
<td>Some guidance issued on roles and responsibilities, but incentives and measures are lacking to ensure accountability.</td>
</tr>
<tr>
<td><strong>GREEN</strong></td>
<td>+1</td>
<td>Leadership at all levels of the delivery chain is in place, understood and resourced; backed by incentives and performance management. Strategic and delivery leadership are clearly distinguished and in place.</td>
</tr>
</tbody>
</table>

**SCORE**

11. Are mechanisms in place for regular feedback and review supporting continuous learning?

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RED</strong></td>
<td>-1</td>
<td>Nothing in place to promote feedback. No facility to disseminate examples of good practice.</td>
</tr>
<tr>
<td><strong>AMBER</strong></td>
<td>0</td>
<td>Guidance filtered down, but no mechanisms to communicate feedback from delivery level upwards.</td>
</tr>
<tr>
<td><strong>GREEN</strong></td>
<td>+1</td>
<td>Frequent feedback between all delivery chain levels. Feedback reviewed, and guidance and examples of good practice shared.</td>
</tr>
</tbody>
</table>

**SCORE**
12. Have systems to achieve efficiency been built into the delivery chain?

| RED  | -1 | Assets and services not shared. High administration costs due to lack of innovation, internal review and challenge to working practices. |
| AMBER | 0 | Opportunities to increase economies of scale not fully realised. Some asset and service sharing. Scope to further reduce transaction and administration costs. |
| GREEN | +1 | Early engagement from key partners when designing delivery chain. Asset and service sharing where suitable. Front line configured to best deliver services. Customers are encouraged to use the most cost-effective delivery channels. |

Commissioned by Zurich Municipal in association with