cloud computing:

how to successfully contract for cloud services
Cloud Computing | how to successfully contract for cloud services

contents

03 | executive summary
04 | the cloud: background, benefits and possible risks
05 | the cloud is not a panacea
06 | cloud contract terms: what are you signing up to?
07 | example cloud contract terms
08 | a typical cloud procurement scenario
11 | how can you avoid procurement pitfalls?
12 | managing the risk in your cloud contract
13 | conclusion
14 | appendix a - cloud types and services
15 | appendix b - about best practice group
executive summary

More and more organisations are becoming interested in cloud computing and making it the backbone of their IT strategies. The financial and technical case for migrating to the cloud is often so compelling it appears an easy decision for the Board.

However, the cloud is in its relative infancy and many buying organisations are still feeling their way into how to set up effective contracts and commercials for the cloud. They are also finding out – often too late – that when the benefits and returns they expect are not delivered, there is very little they can do about it. Fixing the service or exiting the contract is not as straightforward as anticipated and the buyer can find itself carrying much more liability than it expected.

This paper considers the pitfalls you must look out for in cloud providers’ standard contract terms. It also explains how the procurement process has a significant effect on your ability to realise benefits from the cloud, and how you can ensure that you are not assuming all the risk of using cloud services.

How to read this paper
For ease of use, we’ve split this paper into a number of sections, so you can go straight to the content that’s most relevant to you:

- **Background Benefits and Possible Risks of Cloud - refer to page 4**
  For some background on the growth in cloud computing, this chapter highlights the benefits of adopting it and the issues with doing so.

- **Cloud Contracts - what are you signing up to? - refer to pages 6-7**
  From a commercial and contractual perspective, the cloud is still in its infancy. Be careful what you sign up to; this section highlights some of the key terms you need to be aware of.

- **A Typical Cloud Procurement Scenario - refer to page 8**
  Key steps within a common cloud procurement process and the effect

- **Procurement: Route Cause Analysis - refer to page 10**
  A review of the procurement process, setting out the pitfalls and how you can avoid them.

- **How to Successfully Procure Cloud Services - Putting it Right - refer to page 11**
  Managing the risk in your cloud contract is fundamental. Does the risk in cloud computing lie with you or with your provider?

- **Comparative Risk Assessment - refer to pages 12**
  At a glance risk assessment of whether you or your provider owns the risk in the cloud.
the cloud: background, benefits and possible risks

To understand the cloud’s appeal, it’s worth looking at the drawbacks of more traditional approaches to IT.

The on-premise computing model sees organisations employing an internal IT function which looks after and hosts an IT estate. Minimising risk and ensuring enough capacity requires numerous over-specified servers that need considerable upkeep. Internal IT is also responsible for data and network security, helpdesk, disaster recovery and business continuity, technology refresh and IT’s strategic application. This adds up to a considerable cost which is often disproportionate to the benefits, particularly if the budget is spent keeping the lights on rather than moving the business forward.

Driven by these factors, organisations often outsource their IT support to specialist “managed service” providers. This can entail moving the servers off site and migrating to the provider’s data-centre, or maintaining the IT estate internally, but outsourcing the function.

Outsourcing does not always deliver on its promise. Companies often outsource a problem before they fix it internally, creating greater problems down the line. TUPE’s complexities mean the organisation can be left with its existing team and its costs, while losing control of them and paying a management fee. Companies can also find themselves with an inflexible service and large unexpected costs, leading to a breakdown of trust and a feeling of being ‘ripped off’.

The cloud: virtual, scalable and available everywhere

The cloud promises to remove those drawbacks. Every computer needs a network, storage, processor and memory, and every application needs a computer to run on. However, these do not need to be individual, physical machines. Organisations can create numerous “virtual machines” on a single, very powerful, physical server and run each core application on a virtual machine. These servers can be housed in large, highly secure and resilient data centres, and each server can be used by more than one organisation.

This means that organisations can:

• have far fewer physical servers and can increase their utilisation, saving space and cutting their carbon footprint
• enjoy simpler, more reliable and more flexible IT
• access data from anywhere on many devices (including those belonging to individual users), rather than being restricted to desktops
• allow IT staff to focus on delivering IT’s strategic benefits
• benefit from the service provider’s built-in disaster recovery, business continuity, backups and restore points
• employ better technologies for monitoring servers and managing capacity, and remove the limitations created by firmware issues and software updates
• move entire virtual machines between data centres without human intervention.

In effect, virtualisation creates the potential for the cloud to become the fourth utility. Users can scale their demand up and down automatically and be charged for what they use, in the same way that consumers currently access gas, electricity and water. Users avoid the high upfront cost of investing in their own IT structure, replacing it with a small initial investment and low ongoing operational expenditure.
Cloud Computing | how to successfully contract for cloud services

the cloud is not a panacea

There are several ways that cloud provision can be structured, ranging from private clouds for the use of one organisation to public clouds that are accessible to everyone. Buyers can also choose the type of cloud service they want – the infrastructure only, a development platform or a full range of software. Appendix A contains more information about the variety of cloud services available and who they will suit.

As with any service, the cloud comes with its own set of issues. Can you be sure, for example, that your data is always going to be secure and accessible? By using the cloud, you are effectively losing control of business-critical systems, making you entirely reliant on your service provider and on having a reliable internet connection.

Lack of standardisation means that your data can become locked in with your current provider, making it harder than expected to change. The cloud industry is also in its infancy, meaning that more issues may emerge as take-up rises.

There are two other significant issues, which we will explore in the following sections:

1. Users need to be very careful about the contracts and commercial terms they sign up to. These can weigh heavily in favour of the service provider, meaning that the cloud’s expected benefits are more difficult to realise.
2. Buyers have to ensure that they procure cloud services in the right way, so that they get the outcomes they want and don’t end up bearing all the risk.
**cloud contract terms: what are you signing up to?**

**From** a commercial and contractual perspective, the cloud is still in its infancy. This means there is little case law to show how courts will interpret cloud contracts or the extent to which providers will seek to rely upon the express terms of the contract. Suffice to say, it would be very unusual for a provider to concede any express term that is in its favour, unless told to do so by a Court. Queen Mary University of London has conducted the Cloud Legal Project (CLP), a review of 31 sets of cloud provider standard terms. Some of the key findings are set out below. Real-life examples of cloud contract terms are shown on page 7.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Findings</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. You are still responsible for data confidentiality and integrity</td>
<td>Improved physical and data security is a key driver for moving to the cloud.</td>
<td>In many cloud contracts, responsibility for data confidentiality and integrity is expressly placed on the customer. The contract expressly negates cloud provider responsibility for these fundamental aspects and as the buyer, you cannot contract out of your legal, statutory and industry compliance obligations.</td>
</tr>
<tr>
<td>2. There are no restrictions on where your data is stored</td>
<td>Customers often hold sensitive or personal data, which in the UK is subject to data protection legislation. Public sector bodies are particularly exposed to data protection and freedom of information obligations, including where in the world the data resides.</td>
<td>Many cloud contracts do not specify any restrictions on data location. Even when this option is provided, there is not usually a warranty. Given the nature of virtual machines, files can be moved very easily around the world. Many providers are one part of an overall supply chain, which means that the cloud buyer and the first layer provider have no visibility or control over where transactions and processing take place, where data is stored or who has access to it. Your organisation remains liable for any non-compliance when you outsource or use the cloud.</td>
</tr>
<tr>
<td>3. If there’s a problem, you won’t be adequately compensated</td>
<td>If the service provider’s failure or negligence causes you loss or injury, you need to have adequate compensatory arrangements in place.</td>
<td>None of the contracts offered a refund of charges as a remedy. The best compensation on offer was either service credits or one month’s charges. RBS’s recent problems show how organisations can suffer severe financial and reputational loss when their IT fails them. In the traditional computing model, the risk can be transferred through a combination of process and fit-for-purpose negotiated contractual terms. Cloud contracts are seldom negotiable.</td>
</tr>
<tr>
<td>4. Your provider can unilaterally change the contract terms</td>
<td>Traditionally, contract terms are negotiated upfront and remain in place for the lifetime of the agreement, unless formally varied by mutual agreement.</td>
<td>Many cloud contracts can be varied unilaterally by the service provider by simply posting new terms on their website. It is up to the buyer to keep abreast of such changes. The effect depends upon the changes the service provider makes and the impact they would have on your business. This is entirely outside your control.</td>
</tr>
<tr>
<td>5. You may need to go to an overseas court to resolve a serious problem</td>
<td>If you have a serious dispute with your service provider, you may need to resort to the courts to resolve the matter.</td>
<td>Around half of the contracts studied were governed by US law and gave the service provider their home court as the exclusive jurisdiction to hear any disputes. Fighting an action overseas can be very expensive in money, time and the impact on your business of having to travel to hearings. Aspects of UK law that assist the buyer, such as being able to imply terms into an unfair contract or the ability to challenge unfair express contract terms, may not apply.</td>
</tr>
</tbody>
</table>
example cloud contract terms

Cloud contracts often contain clauses that weight them heavily in favour of the service provider. Some examples are shown below:

You are responsible for protecting your data:

“…you acknowledge that you bear sole responsibility for adequate security, protection and backup of your content and applications............we will have no liability to you for any unauthorised access or use, corruption, deletion, or loss of any of your content or applications.”

Amazon Web Services (Amazon, 2010)

The service provider can decide when to disclose your information:

“You authorise ADrive to disclose any information about You to law enforcement or other government officials as ADrive, in its sole discretion, believes necessary, prudent or appropriate, in connection with an investigation of fraud, intellectual property infringement or other activity that is illegal or may expose ADrive to legal liability.”

Adrive.com (ADrive, 2010)

The service provider requires you to grant them a licence in perpetuity:

“Your Content in our Services: When you upload or otherwise submit content to our Services, you give Google (and those we work with) a worldwide licence to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes that we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content.”

“The rights that you grant in this licence are for the limited purpose of operating, promoting and improving our Services, and to develop new ones. This licence continues even if you stop using our Services (for example, for a business listing that you have added to Google Maps).”

Google Drive (Google, 2012)

You are responsible for ensuring the service will achieve what you want it to:

“Your are solely responsible for the choice and use of the Services (and any results thereby generated) and, as such, it is your responsibility to review and decide whether the Services will meet your business objectives.”

(UK provider of virtual private clouds)

The service provider will not be liable for any losses you incur, however they are caused:

“We will not be liable to you for any loss of profits; loss of anticipated savings; loss of business; loss of opportunity; loss of revenue; loss of time; loss of goodwill or injury to reputation; loss of or harm to data (including corruption to and reinstatement of any data); loss arising from fraud on your Equipment; punitive damages, or any indirect, consequential or special loss or damage howsoever caused and whether foreseeable or not.”

(UK provider of virtual private clouds)

You will have to compensate your service provider if you cause it to incur additional costs:

“You promise to compensate us for any additional costs we incur because of any delay or failure by you to perform your obligations or responsibilities under the Service Contract.”

(UK provider of virtual private clouds)

The contract will exclude terms that would have been in your favour:

“Except as expressly set out in these Terms or in any applicable Service Contract, all conditions, representations, warranties and other contract terms are hereby expressly excluded to the extent permitted by law.”

(UK provider of virtual private clouds)

What are the lessons from this?

It is too early to say whether these contract terms are going to stick and they seem counter-intuitive to the purpose of the cloud. However if the jurisdiction is outside of country, as is often the case, it will cost a great deal to bring an action to find out.

The advice is to be very aware of what you are signing up for and to always bear in mind the principle of caveat emptor - ‘let the buyer beware’.

www.bestpracticegroup.com | 07
To realise the cloud’s full benefits, it’s essential that you procure cloud services in the right way. The following case study illustrates some of the pitfalls and explains how you can avoid them. It assumes that the customer is a major private sector company, which is procuring infrastructure as a service using a private cloud (see Appendix A for more on these terms).

What the buyer wants to achieve
The buyer has three desired outcomes. Achieving these is crucial to determining whether the procurement is a success or failure. It wants to:

1. Move its application software estate from creaking in-house servers to a state of the art data centre, with no impact on the business.
2. Benefit from scalable, robust architecture which will grow with the business, is “always-on”, is accessible by mobile devices and is monitored by the service provider, 24/7.
3. Benefit from multiple layers of cost savings, while providing a much enhanced disaster recovery and business continuity capability.

How the buyer goes about procuring cloud services
The company follows an eight-step procurement process, which it hopes will deliver these outcomes.

Step 1. It creates an invitation to tender (ITT) which sets out information such as the as-is and to-be metrics, along with other objectives such as the ability to scale up and down. It also includes various functional and non-functional requirements.

Step 2. Multiple cloud providers respond to the ITT.

Step 3. The company reviews the tenders and selects on price. It believes this is utility computing and if it doesn’t work out then it can easily exit and transition to another provider.

Step 4. The company and provider sign a standard terms contract, along with the commercial model. The ITT and ITT response is excluded from the contract, on the basis that it is a sales document. The definition of the managed service, reporting and monitoring, the implementation plan and pricing will be confirmed after contract signing.

Step 5. The provider buys the infrastructure and sets it up in the data centre. The infrastructure is based on indicative information – after all it can scale up and down so if there are any mistakes they can be easily rectified. The managed service is for kit and function, up to the operating system level.

Step 6. The provider tests the infrastructure according to its own acceptance tests and confirms to the buyer that all the components look to be working.

Step 7. The infrastructure up to operating systems passes the provider’s testing and is approved as “ready for service”. The buyer pays the set-up fees applicable to the project.

Step 8. The project reaches closure from the provider’s perspective and the start of ongoing managed service delivery. The provider begins invoicing for monthly charges.
Cloud Computing | how to successfully contract for cloud services

What’s wrong with the above scenario?

The interesting thing about this example is that at project closure, the project has been 100% successful for the provider and 100% unsuccessful for the buyer. How?

Success for the provider is to set up the infrastructure ready for service and start billing.

Success for the buyer was a seamless transition and business as usual on the new cloud platform. At project closure, everything is still running on the old server estate and the old IT function is still doing what it has always done. Yet the business has paid significant set-up fees and started incurring the monthly charges for a service which is not being used.

Although the process above is often recognised as industry standard, the chances of hitting the three desired outcomes are zero!

This is a potentially costly situation

While the buyer could switch to another provider, it has already incurred significant set-up fees and may well be left with equipment from the first deal that it is unable to use, unless it took the right steps and negotiated an effective contract with the first provider.

In addition, the current lack if interoperability standards between cloud offerings can mean that the buyer finds itself unexpectedly locked in with it’s current provider.

All in all, it is much better, quicker and cheaper to procure correctly first time.

How did the buyer fail to procure what it wanted?

At each step of the procurement process, the buyer made an important but avoidable mistake. These are outlined on the next page.
### How did the buyer fail to procure what it wanted?

<table>
<thead>
<tr>
<th>Step</th>
<th>Comment</th>
<th>Impact</th>
</tr>
</thead>
</table>
| **Step 1.** The buyer creates an ITT, which sets out information such as the as-is and to-be metrics. | The ITT hasn’t communicated the desired outcomes for the business or articulated the business case that any solution must meet. | If the provider doesn’t know your outcomes then:  
1. How can it deliver against them?  
2. How can it comment on their feasibility?  
This de-couples the business case benefits from the contract at the outset, leaving the buyer carrying the financial and technical risks of fitness for purpose and project success. |
| **Step 2.** Multiple cloud providers respond to the ITT. | This will typically be a sales proposal, followed by a beauty parade. | If the buyer undertakes no pre-contract due diligence and assumes the risk of all the provider’s assumptions and caveats. |
| **Step 3.** The company reviews the tenders and selects on price. | The issue is not usually with what is in the price, but what is excluded from it. | The costs can increase hugely once the actual requirement and staffing becomes known. |
| **Step 4.** The company and provider sign a standard terms contract, along with the commercial model. | This is very common. It means that the buyer goes into things with a “clean” contract. The warranties and obligations contained in such a contract are very light and it is comparatively simple for the provider to discharge all its obligations, whether or not this results in the outcomes the buyer wanted. | In addition to the significant risks of signing the standard provider terms (as discussed earlier in this paper), the contract thereafter becomes a series of agreements to agree. Agreements to agree are not operative contractually and so cannot be relied upon if they are not delivered against. This means the buyer faces a large number of unknowns and is assuming all the risk for their delivery. |
| **Step 5.** The provider buys the infrastructure and sets it up in the data centre. | The infrastructure is based on indicative information – after all it can scale up and down so if there are any mistakes they can be easily rectified. The managed service is for kit and function, up to the operating system level. | The buyer takes on the financial and technical risk that the infrastructure has been mis-specified. If the provider’s obligation is to monitor up to the operating system layer, the buyer must check whether this excludes the virtualisation software layer. If it does, the buyer takes the risk that the solution is fit for the applications. |
| **Step 6.** The provider tests the infrastructure according to its own acceptance tests and confirms to the buyer that all the components look to be working. | If this is a series of ‘green light’ tests to show the hardware and network is performing as it should, it is not geared to proving the buyer’s desired outcomes have been achieved. | Once something is accepted, the buyer’s express contractual rights for non or partial delivery generally evaporate. |
| **Step 7.** The infrastructure up to operating systems passes the provider’s testing and is approved as “ready for service”. The buyer pays the set-up fees for the project. | Clearly this is all outside of the buyer’s control. | The buyer becomes liable to pay fees and costs before knowing whether or not the architecture is fit for purpose. |
| **Step 8.** The project reaches closure from the provider’s perspective and the start of ongoing managed service delivery. The provider begins invoicing for monthly charges. | The provider has probably at this point discharged all its obligations. It is now up to the buyer to migrate things over to the new architecture. | The buyer will need to set up a new project to migrate to the new architecture, and will be wholly responsible for its success or failure. The buyer therefore retains overall responsibility for achieving the desired outcomes. |
At each step of the procurement process, the buyer made an important but avoidable mistake. These are outlined below:

1. **Compile Comprehensive ITT:**
   - Include your outputs, desired outcomes required and the business case metrics in your ITT.

2. **Ensure Provider Deliverability:**
   - Require all the potential providers who respond to the ITT to confirm whether they can deliver the outcomes and business case, and make this a condition of contract.

3. **Undertake Due Diligence:**
   - Perform robust due diligence on the contract terms and the supplier’s ability to deliver the data centre, architecture and your desired outcomes – including how these will be achieved.

4. **Ensure Fit For Purpose Contract:**
   - Negotiate fit-for-purpose contract terms with more than one supplier, to allow you to compare risk positions as part of the selection process. Take care to have a residual process in place to ensure the contract is fully formed and contains no caveats, assumptions or agreements to agree.

5. **Insist on Pre-Contractual Scoping:**
   - Contract with providers to undertake a pre-contractual scoping of your requirements, outcomes, internal skillsets and resource availability, and to evaluate issues with moving the applications from legacy physical servers to a virtualised environment.
   - Contract for this as advice in the first instance. Agree terms of reference that will ensure that you understand the true risk position and have effective plans for mitigation. Ensure that an overall transition plan is created and agreed, which will take the project through to business as usual on the new architecture. Ensure that the outputs include a commercial model with effective what-if scenarios, so these are fully considered and understood by both parties before committing.

6. **Check Supplier Evidence:**
   - Select a preferred partner who has evidenced that it can deliver to your desired outcomes, to agreed costs and timescales, and is prepared to underwrite this contractually.

7. **Compile Contract Terms and Schedules:**
   - Assemble the contract and schedules, ensuring that:
     i) the contract terms are fit for purpose
     ii) rights and remedies are fitting
     iii) exit and transition are extremely well defined
     iv) acceptance provisions ensure that buyer outcomes will be achieved
     v) payment provisions ensure both parties are incentivised to deliver the same outcomes, and
     vi) no gaps between the contract terms and schedules.

8. **Check the Architecture:**
   - Ensure the provider builds and proves the architecture in the context of what you actually need, to attain “ready for service”.

9. **Prove it Works:**
   - Migrate and prove the business applications on the new architecture.

10. **Test and Train:**
    - Cutover to the new platform.

11. **Achieve Business as Usual:**
    - Ascertain it’s all working on the new platform.

12. **Realise the Benefits:**
    - Make any remaining milestone payments for successful project completion.

13. **Pay the Invoices:**
    - Check you’ve achieved your desired outcomes and ensure your business case is intact.

14. **Reach Project Closure.**
We’ve shown that both the standard contract terms and your procurement process can have a significant impact on your chances of realising the cloud’s benefits. The table below shows how these contracts and your process can transfer all the project’s risks from your provider to you - and conversely how, by following an effective process, you can transfer this risk back to your provider.

### Risk Item
- **Both parties understanding exactly what is required now and maintaining flexibility for the future**
  - **Cloud Without Process - Who Carries Risk?** You
  - **Cloud With Due Process - Who Carries Risk?** Provider
- **Solution being fit for your purposes now and/or in the future**
  - **Cloud Without Process - Who Carries Risk?** You
  - **Cloud With Due Process - Who Carries Risk?** Provider
- **Solution being of satisfactory quality**
  - **Cloud Without Process - Who Carries Risk?** You
  - **Cloud With Due Process - Who Carries Risk?** Provider
- **Adequate transition planning, project management and resourcing, delivery on time**
  - **Cloud Without Process - Who Carries Risk?** You
  - **Cloud With Due Process - Who Carries Risk?** Provider
- **Liability for cost and time over runs, part or total failure**
  - **Cloud Without Process - Who Carries Risk?** You
  - **Cloud With Due Process - Who Carries Risk?** Provider
- **Data migration (in and out), backup and encryption**
  - **Cloud Without Process - Who Carries Risk?** You
  - **Cloud With Due Process - Who Carries Risk?** Provider
- **Data protection**
  - **Cloud Without Process - Who Carries Risk?** You
  - **Cloud With Due Process - Who Carries Risk?** Provider
- **Specialist vendor’s “Duty to Warn” you of known adverse ramifications**
  - **Cloud Without Process - Who Carries Risk?** Badly eroded, if any at all
  - **Cloud With Due Process - Who Carries Risk?** Provider
- **Statutory and regulatory compliance**
  - **Cloud Without Process - Who Carries Risk?** You
  - **Cloud With Due Process - Who Carries Risk?** Provider
- **Compensation for lost benefits and/or direct losses as a result of solution or provider failure**
  - **Cloud Without Process - Who Carries Risk?** Maximum liability is via service credit - generally one month’s charges
  - **Cloud With Due Process - Who Carries Risk?** Provider
- **Misrepresentation or negligence**
  - **Cloud Without Process - Who Carries Risk?** You
  - **Cloud With Due Process - Who Carries Risk?** Provider
- **Chances of getting contract terms to be fit for your purposes e.g. the correct limitations of liability**
  - **Cloud Without Process - Who Carries Risk?** Start Praying
  - **Cloud With Due Process - Who Carries Risk?** Very Strong
Cloud Computing | how to successfully contract for cloud services

conclusion

This paper has considered the issues involved in procuring for one type of cloud offering – infrastructure as a service. Each of the different cloud offerings will have its own considerations, which you need to understand before you procure.

The providers’ typical contract terms are not in your favour. As with any IT or outsourced service, it is essential that you know what you are signing up to and ensure that the risks and rewards are appropriately shared between you and your provider.

When negotiating the contract and commercials, you and your provider must be lined up so that all parties are incentivised to achieve the project outcomes that you define at the outset. This also means aligning the expectations of the teams involved, from your project team to your finance department, to ensure that you achieve your business case. While your provider has responsibilities to ensure a successful project, it is equally important that you play your part too.

Getting the contract and commercials right greatly increases your chances of a successful outcome. You also need expert input and quality assurance during the implementation phase, to ensure that this runs smoothly: while your provider is an expert in these services, buyers are generally not.

how best practice group can help

We are industry leaders at advising on procurement, negotiating contracts and ensuring desired outcomes. With extensive operational backgrounds and detailed knowledge of contract law, we are ideally placed to help you achieve the outcomes you are looking for. We can also draw on a wealth of technical expertise, with specialists in areas such as data centres, the cloud, virtualisation and commercials, as well as our own experience of implementing cloud services in our business.

The breadth of our capabilities allows us to take a holistic view of your project, so we can advise you on everything involved, whether that’s constructing your business case, scoping your technical requirements, designing your managed service, testing your solution to ensure its fitness for purpose or realising the benefits.

If you’re considering cloud services, then talk to Best Practice Group.
There are four primary types of cloud – public, private, community and hybrid, which is a mixture of both public and private.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private Cloud</td>
<td>A cloud which is dedicated to your organisation, whether on-premise or off-premise - it sits behind your firewall.</td>
</tr>
<tr>
<td>Community Cloud</td>
<td>A cloud infrastructure shared by several organisations who have a common interest or security requirement such as police, hospitals, security services and universities. This may be on- or off-premise and managed by the organisations or by third parties.</td>
</tr>
<tr>
<td>Public Cloud</td>
<td>Cloud services open to all and owned or managed by the organisation selling the cloud services.</td>
</tr>
<tr>
<td>Hybrid Cloud</td>
<td>Made up of two or more of the above, for example a combination of on- and off-premise clouds, which are linked.</td>
</tr>
</tbody>
</table>

The diagram below summarises how the various types of cloud interlink. There are important cost-efficiency and security factors pertaining to each, which are subjects in their own right. BPG can provide you with more information on the risks and issues of each type of cloud.
There are three primary types of cloud available as a service: infrastructure, platform and software.

<table>
<thead>
<tr>
<th>Cloud Offering</th>
<th>Description</th>
<th>Of Interest To</th>
<th>Primary Features &amp; Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure as a Service (IaaS)</td>
<td>Provision of the core infrastructure, commonly up to operating system level.</td>
<td>Enterprises who wish to reduce their reliance on internal computing infrastructure</td>
<td>Scalable, Elastic, Pay as you go, Best of breed technology and resources at a fraction of the cost.</td>
</tr>
<tr>
<td>Platform as a Service (PaaS)</td>
<td>Pre-configured platforms to develop, test and run software and apps. Examples include Force.com, Microsoft Azure, Apple OS and iOS, Google apps engine.</td>
<td>Primarily software developers</td>
<td>Developers can get on with developing their applications, rather than worry about setting up all the environments and supporting applications and components.</td>
</tr>
<tr>
<td>Software as a Service (SaaS)</td>
<td>Application software running in the cloud and accessible via mobile device and/or web browser. Includes email services such as Gmail, and a vast array of business-focused apps such as CRM, financials, ERP, office and productivity software.</td>
<td>Potentially everyone</td>
<td>Monthly pay-as-you-go rather than big up-front licence costs, Reliable and scalable infrastructure, Mobility - can access applications while on the move, Much faster deployment - already set-up.</td>
</tr>
</tbody>
</table>

how it all stacks together

The diagram adjacent shows how the different cloud deployment and service delivery models described above come together:
The principals of BPG – Allan Watton, Richard Kerr and Chris Browne – and their associates have worked on more than 500 projects between them in organisations throughout the public, private and third sectors. These have included some of the best known blue-chips, such as Lafarge Industries, Kingspan Holdings and Scottish & Newcastle. Public sector organisations include county, unitary, city, borough and district councils, plus NHS, charities and central government organisations. If you want to discuss any issues, or simply have an informal conversation with someone to bounce ideas off, please call Judith Bohren on 0845 345 0130 or email advice@bestpracticegroup.com and she will advise you about available time and date slots.

For over a decade, BPG has served as a trusted independent business advisor, helping commercial and public sector organisations to reduce the cost of working with major strategic outsourcing, joint venture and technology service providers.

Principally, BPG does three key things. We:

• Help clients find the right service provider in the first place, ensuring the services delivered meet the organisation’s required business outcomes, that costs of delivery are minimised and relationships between the vendor and the client are optimised.

• Improve the performance of existing vendors while producing direct cashable savings and dealing effectively with conflict resolution.

• Minimise risk and cost and ensure service levels are maintained while an underperforming vendor is replaced.

Why do organisations need specialist assistance?

• Research from the British Computer Society, Gartner Group, Standish Group, Butler Group, Kable Group, KPMG, Technocrati and others concludes that between 56% and 87% of major projects fail outright within two years of commencement, going over double their budget and implementation timescales.

Why are BPG’s advisors more effective?

• Extensive operational expertise. They are ex-CIOs, IT directors, service directors/managers and business process re-engineering experts.

• Most of our advisors have also read, implemented and/or practised contract law in live commercial environments.

How does this make BPG unique?

• Hands-on operational and contractual expertise.

• Specialist combined operational and contractual expertise helps us align contractual terms to the business outcomes and operating relationships expected of service providers.

• The war wounds of over 500 projects that we have been asked to rescue after the event.

What does this expertise mean for my organisation?

• Project costs are significantly reduced.

• Business outcomes are achieved twice as fast – see the comments from our clients on http://www.bestpracticegroup.com/testimonials

• Excellent operating relationships are forged with your service providers – working in true partnership.

• Working to our strengths, we deliver excellent outcomes in half the time of other practices.

• By our helping to coach your own people, you can achieve these benefits for your own organisation.
clients who have benefited from BPG’s services

BPG and its associates have advised on over 500 projects across more than 200 clients in the public, private and third sectors.

It has worked with both large and small organisations across the UK and Ireland.

Some example larger private sector organisations

- Filofax
- WBB Minerals
- GKN Aerospace
- Dunelm Mill
- Glass Guide
- Kingspan
- Scottish & Newcastle

Some example larger public and third sector organisations

- Orbit Group
- Tullis Russell
- Lafarge
- G4S
- Action for Children
- Scope
- Sustrans
- Cumbria County Council
- Brighton & Hove
- Hampshire County Council
- Oxford City Council
- States of Jersey
- Essex County Council
- NHS
- City & Guilds
- Remploy
- Northern Ireland
- Durham County Council
- Royal Palace of London
- Houses of Parliament

www.bestpracticegroup.com | 17
If you’re considering maximising the value you achieve from your strategic provider partnerships, talk to Best Practice Group.