The cloud: A buyer’s guide

Everything you need to know
and consider before moving to the cloud.

An ebook by

HighQ

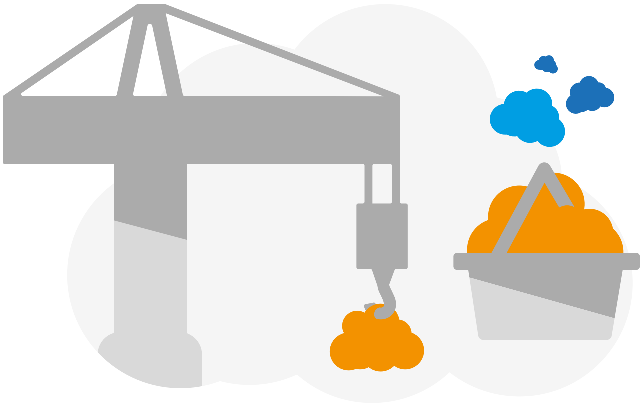
highq.com

Secure, social, cloud

Mutually exclusive or perfect partners?

Buy vs Build

The pros and cons of cloud software



10 Questions to ask your cloud provider

Secure, social, cloud

Mutually exclusive or perfect partners?

This chapter looks at two of the hottest topics in technology today – social software and cloud computing – and asks whether cloud-based social software is inherently risky for enterprises looking to take advantage of the new wave of technology innovation or whether it is possible to have your cake and eat it.

In the last five or so years, enterprise social collaboration software and cloud computing have both transitioned from the fringes of corporate IT policy to become serious business priorities. The benefits of cloud computing and software as a service in particular are generally well accepted and represent an effective way for organisations to reduce the costs associated with running their own data centres and developing applications in-house.

Can you have your cake and eat it?

In addition, the adoption of enterprise social tools is increasingly seen as an effective way of improving workforce productivity, communication and knowledge sharing both internally and externally. This is often characterised simplistically as "Facebook for the enterprise" and usually involves some combination of secure file sharing, blogs, wikis, microblogs, task management, people profiles and activity streams. Software as a service providers like Salesforce and Google have paved the way for organisations to embrace the cloud as an alternative to developing and hosting traditional enterprise software on-premise. The cloud offers cheap, scalable computing resources and software on demand without the need for companies to build out their own data centres or develop their own applications.

In theory then, enterprise social software hosted in the cloud should be the perfect combination of two of the hottest technology trends and give organisations immediate access to the latest wave of innovative software with no development resources or capital outlay necessary.

But is the cloud secure?

In reality, the problem for a lot of organisations comes when it's time to actually move their software and data to the cloud. There is often resistance at senior levels and a concern around the security of data hosted outside of their network.

Much of the concern around security is born out of misconceptions about the cloud and software as a service in general. There is often an assumption made that cloud providers are less secure than hosting inhouse in your own data centre. There are of course various types of cloud services and not all of them are targeted at the enterprise.

Consumer-grade services like Dropbox or iCloud are probably not the best places to store your sensitive corporate data but at the other end of the spectrum there are specialist providers who build enterprise-grade services specifically for those industries where security and control are paramount, such as the legal, banking, life sciences and government sectors.

These specialist providers often have their own private clouds and do not rely on public cloud providers like Amazon or Microsoft for hosting. They are advanced technology companies and their businesses depend on running secure and dependable services for high value clients. Their clients will audit them and require proof that their systems and services are secure via software penetration tests and adherence to information and security standards such as SAS 70 Type II or ISO 27001.

A law firm, bank or corporation is not primarily focused or dependant on providing a state-of-the-art technology platform. Whereas, a cloud provider is only able to stay in business if it has the trust of its clients and it can only do that by maintaining a robust, reliable and secure service. So it stands to reason that in order to win clients and then keep them, a specialist cloud provider musthave at least as good security measures in place, if not far better, than the vast majority of organisations have themselves.

Does social mean insecure?

The second thread of resistance to the implementation of cloud-based social software is to the very concept of “social” itself. There is a common belief that “social” cannot be secure because it is based on the concepts of openness and sharing. It is also often perceived as a time wasting activity with no business benefit.

This couldn’t be further from the truth. The best enterprise-grade social tools have robust and advanced controls that enable you to share information and collaborate with other specified users inside and outside of the organisation in a secure way. You choose exactly who to share your information with and it can be as open or as closed as you like depending on what you are sharing and who you are collaborating with. Users can be given various levels of privilege and access, from full administrator rights to a read-only view on an individual content item.

So what does it mean?

What “social” really means is emphasising people and connections rather than just data. Being able to see who authored or shared a piece of content can be as valuable as the content itself. Enterprise social software is about enhancing communication, collaboration, and knowledge sharing. It enables users to make the connections and have a peripheral vision of the work going on around them with their colleagues, partners and clients internally and externally so that they can be more effective and productive.

So, I can have my cake and eat it!

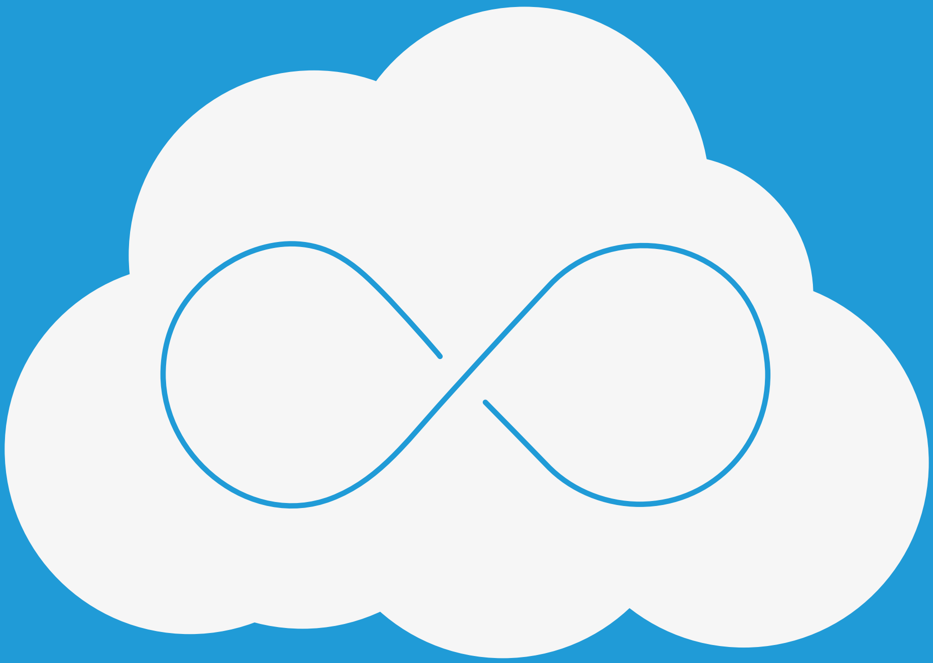
Yes you can.

Cloud-based social software is no less secure than a document management system, email or talking to someone by the

water cooler but it can be a lot more effective at capturing, storing and then quickly redistributing information to the parts of the business where it is needed the most. Not all information in an organisation can be shared openly but in an enterprise-grade social system you have the opportunity to do so when it's appropriate and keep it locked down and secure when it isn't.

Social software and the cloud is like anything else, you need to look at all of the options and choose wisely. Do your due diligence, ask the difficult questions, speak to existing clients of the provider and ask them why they chose that solution. If you're not comfortable with hosting your data in one of the big, public cloud platforms, look for a smaller, more specivalist provider. You will probably get a more personalised service and solutions tailored to your industry or use case.

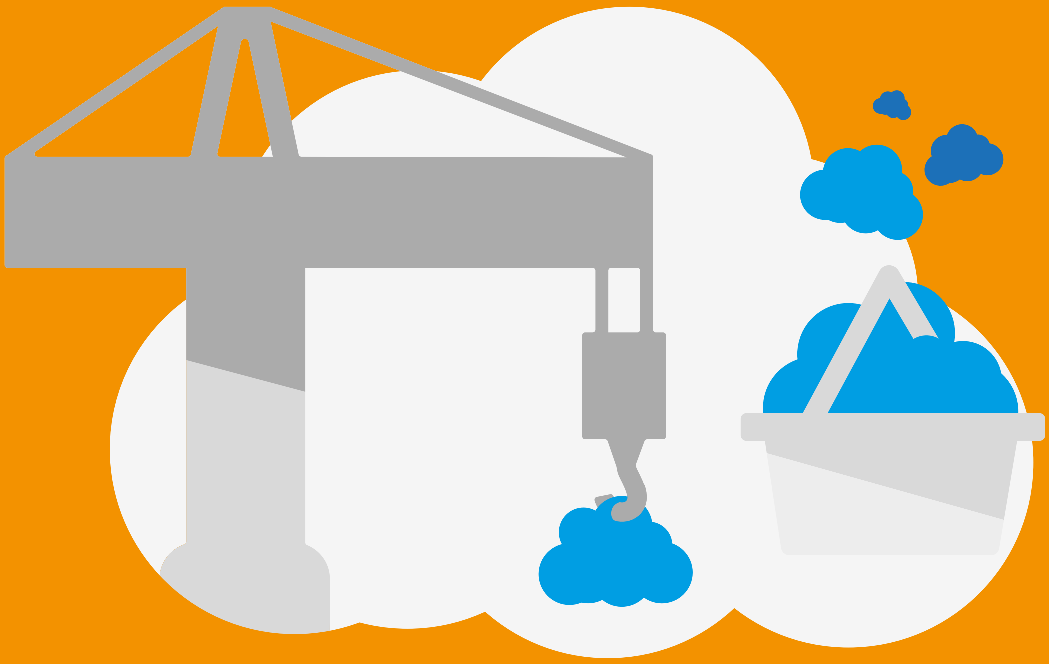
But remember, whilst there is nothing inherently insecure or risky about software as a service or social tools in comparison to traditional solutions, they can still be poorly implemented, abused and suffer from a lack of governance. However, if you choose the right cloud solution and implement it well it can lead to significant cost reductions, gains in efficiency, much more flexibility and access to cutting-edge technology that would otherwise take years to implement.



Collaborate

Software as a service providers like Salesforce and Google have paved the way for organisations to embrace the cloud as an alternative to developing and hosting traditional enterprise software on-premise. The cloud offers cheap, scalable computing resources and software on demand without the need for companies to build out their own data centres or develop their own applications.

Find out more by clicking here



Buy vs Build

The pros and cons of cloud software

In these tricky economic times with downward pressure on internal budgets, alternative feearrangements and an expectation from clients to deliver ever more value, there are difficult decisions to be made about the best way to provide new client facing services. This inevitably involves technology and needs to be put in place quickly and efficiently. Until fairly recently, the installation of new systems has required an army of developers, system administrators, additional data centres, a long lead time and large budgets to build and run applications in-house. Now off the shelf cloud-based software offers a real alternative that has some potentially massive advantages.

Own vs Rent

Often the debate around cloud computing is simplified into a Capital Expenditure (CapEx) versus Operating Expenditure (OpEx) debate. This is an important consideration but there is more to it than that. The real question is about whether a firm needs its own software and the infrastructure it runs on, or it can simply rent it.

With software as a service, firms are effectively renting it for a period of time (usually a year for enterprise software) and after that year, a firm can either switch to something else or continuing using it for another year. The real difference with building and managing your own software inhouse is that firms are making a long-term commitment and investing in it up front. For many, this can make it harder to be flexible if requirements change. It also significantly increases the costs of switching to another solution down the line.

Cloud-based software is available immediately off-the-shelf with virtually no lead time and is constantly evolving and being upgraded. It means the customer is always using the latest technology without any additional effort. If the customer doesn't like it, they can simply switch to another provider because they're not tied to it for the long-term.

Own vs Rent

A good analogy is that of buying a car outright or leasing it on an annual basis. If you buy it, you have to fund the full-value of the car in one lump sum and then you are responsible for maintaining and servicing it for its entire lifetime, or at least until you sell it. After five years, it will have depreciated significantly and be out of date compared to the latest models available.

If you lease the car instead, a service and maintenance contract is normally included and at the end of each year you can upgrade to the latest model or switch to another car entirely and you don't need to find any up front cash to buy it.

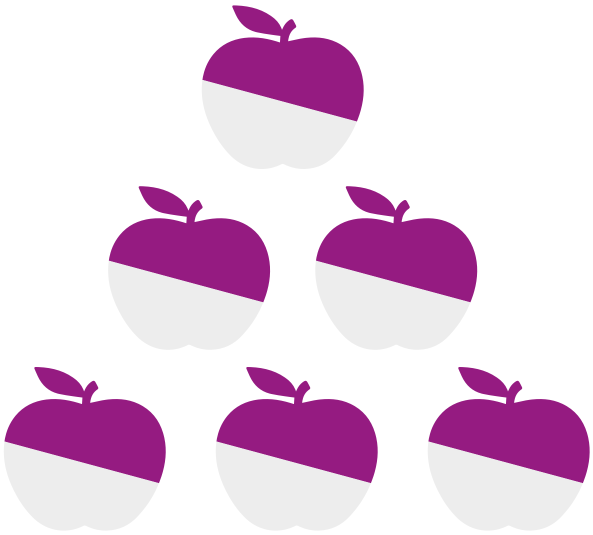
Going back to technology, the best option for an organisation depends on its culture and the nature of the software or service. However, you don't need to look very far these days to see the increasing number of companies that are moving key business software into the cloud for email, document management, client relationship management (CRM), extranets and even intranets.

Compare apples with apples

A good analogy is that of buying a car outright or leasing it on an annual basis. If you buy it, you have to fund the full-value of the car in one lump sum and then you are responsible for maintaining and servicing it for its entire lifetime, or at least until you sell it. After five years, it will have depreciated significantly and be out of date compared to the latest models available.

If you lease the car instead, a service and maintenance contract is normally included and at the end of each year you can upgrade to the latest model or switch to another car entirely and you don't need to find any up front cash to buy it.

Going back to technology, the best option for an organisation depends on its culture and the nature of the software or service. However, you don't need to look very far these days to see the increasing number of companies that are moving key business software into the cloud for email, document management, client relationship management (CRM), extranets and even intranets.



Focus on delivering business value

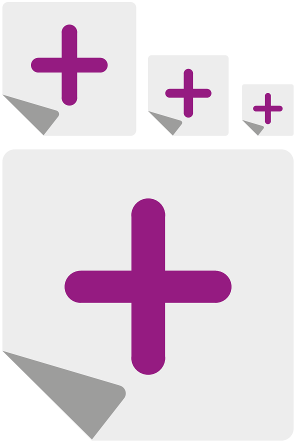
Ultimately, technology is just an enabler for an organisation to do business and provide a service to its clients. It's easy to lose sight of this simple fact and look at technology as a differentiator and the key to a competitive advantage.

The reality is that technology is increasingly commoditised and at the same time becoming ever more sophisticated. This means it's a lot harder for any organisation to truly differentiate itself based on technology. A specialist technology vendor will be able to do the same thing more quickly, cheaply and effectively than you and will sell it to all of your competitors for a much lower price.

What really differentiates a professional services organisation is the service it provides, its specialist knowledge and its experience. Clients don't care whether firms deliver that via the same software as competitors. They just focus on the firm's output.

Most organisations, particularly those in the same industry vertical, have very similar requirements. Imagine if every company built their own email or word processing software. Would that make sense? The same is true of virtually all desktop or cloud software these days.

The best way to deliver real value is for organisations to roll-out technology that is swift and agile. It needs to respond to the business's requirements quickly and enable it to provide its clients with the best possible service. Cloud-based software does this by enabling rapid deployments with constant upgrades and improvements. Spending considerable time and money building in-house software is not a good use of scarce IT resources. We believe it is much better to let software vendors take care of that so that firms can focus on being the best at what they do.



Watch a video

Cloud-based software delivers value by enabling rapid deployments with constant upgrades and improvements. Spending considerable time and money building in-house software is not a good use of scarce IT resources. We believe it is much better to let software vendors take care of that so that firms can focus on being the best at what they do.

Click here to learn more about collaboration software

10 Questions to ask your cloud provider

Office virtualisation and web-based applications are attractive for a number of reasons, not least because of the scalability of the cloud, the reduction in burden on IT staff and the fact that it should save time and money.

With the advent of flexible working practices and remote working, it is not hard to recognise the value of adopting a cloud approach to IT infrastructure and applications. But how should enterprises address the myriad of cloud options and what questions should they ask their provider before taking this important step? Here we have outlined some of the most important questions. time and large budgets to build and run applications in-house. Now off the shelf cloud-based software offers a real alternative that has some potentially massive advantages.

Are they audited? 1

ISO 27001 is the information security standard that most customers will look for. There are numerous other auditing and accreditation measures that indicate whether the provider meets high levels of physical security and internal control, as well as having a strong commitment to data security.

Ask the provider what accreditation it holds and how this matches against other well-established vendors. Customers should also consider having independent penetration tests for additional peace of mind.

Are they financially healthy? 2

Naturally it's important to choose a cloud provider that is financially stable and not likely to go out of business. IT contractor 2e2 went bankrupt in January 2013 leaving its data centres in jeopardy and many of its customers in a state of anguish. With proper due diligence, a customer can ensure that a cloud provider's financial health is secure and that its services will not be interrupted or fail entirely.

Where is my data? 3

Customers should consider the location of data centres and whether they may be at risk of flood, earthquake or other natural disaster. Data centres should also be located in a politically stable jurisdiction. Customers should think carefully about where their data is being stored. America's PATRIOT Act has led some cloud customers to avoid using data centres on US soil for fear of US law enforcement's attempts to intercept communications.

Data centres outside of the US that are owned by US-based cloud providers may also fall under the reach of the PATRIOT Act. The UK's Regulation of Investigatory Powers Act (RIPA) has also raised similar concerns, although many commentators suggest that fears concerning UK and US legislation have been over-inflated. If either of these Acts are a concern, ask your provider if they have offshore hosting in other jurisdictions that may not be subject to the same regulations.

What happens if their servers fail? 4

Deploying cloud components in different locations should prevent customers from suffering from an outage at one specific facility. Any enterprise-grade cloud vendor should also have full data centre failover and disaster recovery in place to prevent any failure of one centre taking out the entire service. Amazon Web Services suffered an outage at its Northern Virginia data centre in December 2012, but customers that had adopted a cloud model involving multiple data centres suffered little or no ill effects.

Customers may decide to store files in multiple locations at geographically dispersed data centres and copies of these files should be updated and synchronised automatically. If one data centre suffers an outage, this should not be a major problem for the customer.

Customers might consider a data centre site visit. They should estimate the true impact on the business in the event of a failure and identify what the vendor's likely recovery time would be. There should be an opportunity to test the disaster recovery plan and to iron out any obvious deficiencies.

Customers should ask the provider about how clients are prioritised when attempting to bring them back online and whether a premium could be paid to ensure that they are given precedence. Customers will want to think about whether a contract can be terminated in the event that the provider is not fulfilling its contractual obligations and how easy it will be to transfer to an alternative provider.

How is my data secured? 5

Discover how many security personnel are involved in monitoring the data centre and who is actually allowed into the data centre. What security processes exist to ensure that access is only provided to authorised individuals? What sort of firewalls and detection systems are in operation to guard against malicious network activity or system attacks? What is the response plan in the event that security or firewalls are breached?

How are connections secured? 6

Customers will want to employ high-grade encryption technology to ensure that data is not compromised in transit between device and data centre. They should discuss with the cloud provider how to revoke access to files and folders and whether a user's account can be disabled instantly in the event that a device is lost or stolen. They will want to ensure that firewalls are constantly preserved and are not compromised by nonauthenticated sources or unencrypted data.

Do they guarantee uptime? 7

According to the International Working Group on Cloud Computing Resiliency (IWGCR), the average downtime is 7.75 hours a year. The group suggests that since 2007 there has been 1300 hours of downtime at 28 major cloud providers, which it estimates as having an economic impact of $273.3m (stats correct June 2013).

Customers should ask about the uptime guarantees and the service level agreements (SLAs) offered by the vendor. You will want to know what the exclusions to uptime guarantees are in the SLA and what happens if the system is running too slowly and workers are not able to perform their daily tasks as normal. Customers should ask their provider what constitutes an act of God or "force majeure". A narrow definition would be preferable.

SLAs will often provide for credits in the event that service levels have been missed, but often this does not compensate for actual business losses. Customers should check whether the provider is satisfactorily insured so that they can be properly compensated in the event of downtime.

Who can access the data? 8

While it is commonplace for SaaS providers to retain some access to your data to assist with support when required, there are others who may have access to your data. Do support staff at the data centre have direct access to the data processing hardware and if so, are these accesses audited by the provider? Is support staff access to your data audited and can you access these logs easily along with the audits of your own users access to the system?

Will I be sharing servers? 9

If a client is adopting a shared facility they should ask how their data is isolated from other customers' data. Is the service single-tenancy or multi-tenancy? Is it hosted in a private or public cloud? It is advisable to have a detailed description of the virtualisation process and how data is segregated from other clients.

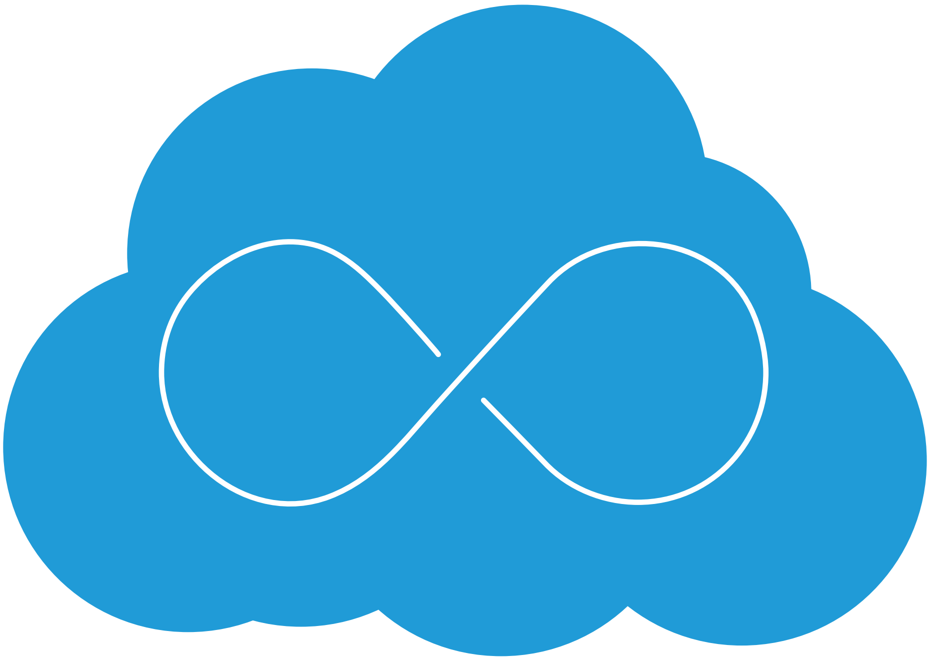
If customers do choose dedicated infrastructure, they should still ask their cloud provider whether there might be less sensitive elements of their systems that might be better suited to a less-expensive multi-tenanted platform. Customers may also have the option of owning the infrastructure and this could be recovered in the event that the cloud provider goes into bankruptcy or does not fulfil its contractual obligations.

Can the platform grow with me? 10

The cloud model is supposed to be elastic. It should allow for business growth or contraction as well as spikes in business activity. Customers should ensure that the provider is able to accommodate these likely events and be transparent about the associated costs.

A final suggestion

Customers should take up references and understand the processes that other clients have gone through to achieve a satisfactory cloud solution. Often an existing customer can better answer these questions or concerns.



Request a free demo today

Follow the link below and sign up for a free demo of HighQ Collaborate.

Find out why Collaborate is the perfect blend of secure file sharing and social collaboration tools, and how it can help your business in infinite ways.

Request a demo or find out more information

HighQ