simmons+simmons

Cloud Services

Setting your strategy

Overview

Cloud services have become an important part of information technology delivery for organisations over recent years. In their various forms, they have proved versatile and agile and, despite initial reservations in some quarters, they have gradually become mainstream across all business sectors, even where information security, confidentiality and regulatory compliance are critical.

The essence of cloud services is the provision by the supplier of an IT service to its customers which is hosted on external infrastructure ("in the cloud") and delivered by way of an internet connection. As a result, the customer is able to access relevant hardware and software services remotely rather than having to buy and install software and maintain equipment itself. The cloud in which the various services are hosted may be public, private or a mixture of the two; each brings its own advantages and disadvantages and it is essential to take these into account when selecting cloud services.

Cloud services are evolving rapidly, and industry experts believe that this trend will continue into the future. Gartner, Inc predicts strong growth in the worldwide public cloud services market to total $332,723 million in 2019, with cloud system infrastructure services and cloud advertising growing the fastest (Source: Gartner, Inc press release, February 2017). Any organisation that is considering moving its IT provision to the cloud, or expanding its current offering, needs to understand the market and take steps to address the risks involved in cloud adoption, particularly if they operate in a regulated area or handle large volumes of data. This guide sets out our approach to helping you to establish and refine your cloud strategy. If you would like to find out more, please see our additional guides, Cloud Services: contracting guidance and Cloud Services: a practical guide to regulatory considerations for Financial Institutions, Asset Managers and Investment Funds.

Source: **Gartner**, Inc press release, February 2017

How can we help?

We are ideally placed to help you to navigate the challenges that developing and implementing a successful cloud strategy presents as:

We have a combination of customer and supplier-side experience. This means that we have a detailed understanding of where each party's areas of sensitivity may lie and of market norms

We specialise in four client sectors – Financial Institutions, Technology, Media & Telecommunications, Asset Management & Investment Funds and Life Sciences. This means that we have a deep understanding of the regulation and pressures affecting these heavily regulated sectors

We have recent experience on advising major institutions on their internal cloud contracting policies and on cloud services arrangements with the largest suppliers such as Microsoft, Oracle, Workday, Salesforce and others, which means that we can help you to get to the point quickly with those suppliers.

We have supported a significant number of clients in regulated industries on multi-jurisdictional due diligence associated with cloud rollouts and have provided quasi-in-house support on implementing associated compliance measures

simmons+simmons

The structures and models explained

To exploit the potential advantages of Cloud Services, it is essential, as a customer, to understand the market and carefully select a solution which best meets your business strategy and processes. Fundamental to this is an understanding of the various models.

Public

The cloud infrastructure is shared by all subscribers. This can be a very cost-effective model and quick to implement but, in order to maximise the number of potential customers, it is heavily standardised. Communication is over the public internet.

Private

The infrastructure can be accessed by the subscriber only. In shared data centres, resources are segregated to preserve privacy. This model enables the service to be tailored to individual needs. Communication takes place over the public internet, a dedicated network or VPN.

Hybrid

As its name suggests, a hybrid cloud environment combines public cloud and private cloud. The infrastructure remains separate but allows data and applications to be shared between the two. This model is often used where some applications or datasets are more sensitive than others.

Community

The infrastructure is shared by a number of organisations with common concerns or requirements, typically security, privacy, performance and compliance. Examples include government departments, banks and airlines.

The services offered fall into three basic categories: Software as a Service ("SaaS"), Platform as a Service ("PaaS") and Infrastructure as a Service ("IaaS").

SaaS

The supplier remotely hosts and manages software applications and provides support services. In many cases the scope for tailoring the services is limited, hence the use of SaaS for fairly standardised applications such as email, helpdesk services, payroll, logistics tracking, customer relationship management and accounting. Increasingly, however, offerings have become more sophisticated and some configuration is possible to meet subscribers' needs.

SaaS offers solutions which can frequently be implemented quickly with limited up-front investment, but concerns for customers include a loss of control, data privacy and how to secure the return of data on termination.

PaaS

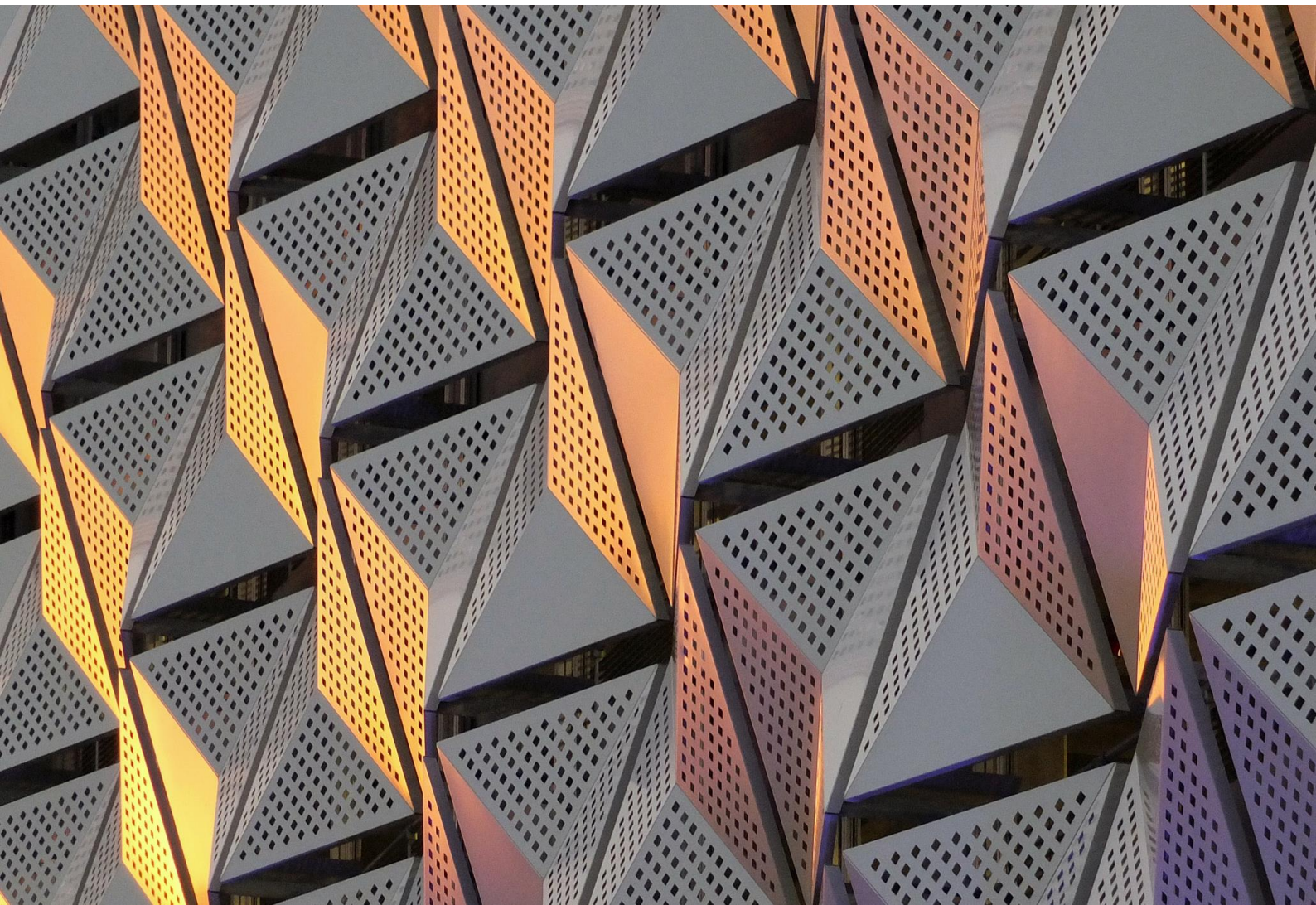
Here, the supplier provides a platform on which subscribers can develop, manage and run applications and operating systems without having to take responsibility for acquiring and maintaining the requisite infrastructure. It is often used for specialised services such as authentication, payment gateways and data access.

PaaS is often a very attractive option for smaller software developers. However, there is a tendency for customers to become locked in; most PaaS platforms are based on proprietary programming interfaces and it can be difficult to change provider.

IaaS

As the name suggests, infrastructure such as servers, storage and networking hardware are hosted by the supplier, sometimes across different data centres. As a customer you are given access to the virtualised components. IaaS is particularly useful for testing and development, storage and recovery, and big data analysis.

Save for complex or legacy systems, a customer's existing workload can usually be transferred to the cloud with only minimal changes. Capacity can be quickly increased or decreased according to need.



What are the key considerations associated with cloud services?

As with other technology and outsourcing projects, adopting cloud services is not without risk and, as always, finding the best solution – or even making the initial decision to proceed – will depend on finding the correct balance and seeking appropriate advice. The key advantages and disadvantages are explained below.

Cost

The cost advantages (and, in particular, potential savings on capital expenditure) are significant drivers for any business considering cloud services. In many cases, suppliers are able to offer cost-effective solutions as a result of economies of scale. From a customer perspective, many organisations with high IT infrastructure costs can make huge savings; adopting a cloud model avoids the need to invest in large numbers of powerful servers and to deploy and maintain them in-house. As cloud services are usually provided on a subscription basis, with regular payments, it is easier to control cash flow and of course, significant capital expenditure (for example, on new infrastructure) is avoided altogether. With the supplier taking responsibility for maintenance, service delivery and availability, you may not need as many in-house IT staff on site, which may further reduce operational costs.

Operational

Cloud services are designed to be user-friendly and as a result, they can be relatively straightforward to roll out across a business, minimising barriers to adoption. The customer is given access to up-to-date (and in some cases, state-of-the-art) technology with new releases and functionality delivered automatically without interruption to the service. Staff can collaborate more easily on projects and documents without the need to email documents, which is very attractive for global organisations or those with a remote workforce. From an IT strategy perspective, adopting cloud services can provide increased storage capacity, improve compatibility between operating systems and web-based applications can improve the performance of users' desktop PCs.

Flexibility

Cloud services frequently allow users to scale up their usage quickly and easily to meet sudden spikes in demand. Likewise, they can be straightforward to scale down again. This makes the cloud ideal if you have fluctuating bandwidth demands or are predicting a period of rapid growth. In terms of business operations, reduced demands on your internal IT team free them up to focus on strategic or bespoke projects which add more value.

Environment

Organisations frequently find their energy requirements fall sharply following a move to the cloud, especially if extensive air-conditioned spaces for servers are no longer needed. This is a consideration for anyone wishing to show a reduction in their carbon footprint as part of a green agenda.

Business continuity

Having your data stored in the cloud can ensure it is backed up and protected in the event of a power failure or other crisis, minimising any downtime. Likewise, using a distributed infrastructure should reduce the risk of disruptive outages. A good cloud-based disaster recovery plan with regular automatic back-ups lowers the risk of data loss or corruption compared with traditional methods of restoring and recovering functionality and, of course, can be accessed from anywhere with an internet-enabled device. However, as well as satisfying yourself about a supplier's disaster recovery processes, it may be sensible to draft your own business continuity plan to accommodate a sudden change of cloud provider. Institutions subject to the EBA's revised Guidelines on outsourcing arrangements will need to have appropriate business continuity plans in place regarding outsourced functions which are considered critical or important.

Connectivity

The connection between the customer and the service risks becoming the single point of failure. A reliable high-speed internet connection will therefore be essential.

Loss of control

Many businesses find it difficult to adjust to no longer having sight of their own hardware and software on their premises. Organisations used to a very bespoke in-house service could well have to rethink their internal processes to make the best use of a more standardised cloud model. If you control a lot of personal data or commercially sensitive information in your business, handing it over to a third party may pose a high operational risk, and such issues will need to be addressed carefully when planning your cloud strategy.

Security

It is often thought that cloud services are inherently vulnerable and more likely to be targets for hackers. Given the negative impact of security breaches, especially in consumer-facing businesses, doubts in this area can be a powerful disincentive to adoption. As technology develops, encryption is becoming ever more sophisticated. There is every incentive for suppliers to invest extensively in this area to differentiate their offerings. Risks can be reduced through appropriate contractual steps such as clearly defined responsibilities and controlled access, as well as technical solutions.

Regulatory concerns

Businesses active in a regulated sector need to be aware that the relevant regulatory body might have specific requirements which need to be considered where cloud services arrangements are proposed. For further details on how this affects the financial services sector as an example, see Page 10.

simmons+simmons

Supplier selection

The pool of potential suppliers is vast and ranges from market giants to small niche players. Choosing a supplier is a key strategic decision, responsibility for which should be shared between senior management and the IT department. Outlined below are several important points to consider before a choice is made.

As a first step, it is essential that you fully understand your own business needs, in particular your technical, service, security, and data governance requirements. This will enable you to identify the efficiencies, gaps, risks and opportunities for change. Once you fully understand your business objectives, make sure your potential supplier does too.

Any supplier should have the appropriate expertise and technical knowhow to provide the services you need. We recommend checking as part of your due diligence that they can deliver adequate levels of service and when they plan to upgrade and develop their offerings. Do they have any recognised qualifications or certifications? Do they have a roadmap for future technology which will foster innovation? Do they really understand your current operations and strategy? Organisations within a specific sector, such as financial services, healthcare or retail, may be wise to identify suppliers with existing knowledge of that field. Also, establish how much work would be involved in migrating to the supplier's platforms as this should be taken into account as part of your business case.

Once you have your short list, we recommend considering the following:

- Business health and profile – are they stable, with sufficient capital, with a formal management structure and risk management policies?
- Reliability – how do they typically perform against their service level agreements? How is downtime dealt with? What sort of disaster recovery processes are in place and what are the recovery time objectives?
- Do they have subcontracts or relationships on which they are dependent for service delivery? A long chain of subcontractors could be unacceptably risky for mission-critical processes or highly sensitive data.
- The various service and pricing models on offer. Each supplier will have different bundles of services and pricing options. Where charges are volume-based or usage-based, it may be easy to exceed budgeted amounts inadvertently at times of high demand. Equally, there may be unexpected add-ons.
- Levels of system security and security governance processes – these should support your own security policy and processes. Can you audit the security arrangements? Does the supplier comply with industry standards, for example the ISO 27000 set of IT security standards, and can they maintain compliance?
- Where are the supplier's data centres – and those of any sub-contractors – located? The supplier should be transparent about this to enable you to assess their data centres and, where necessary, implement associated compliance measures (such as in relation to data protection). You might also want to choose locations which are stable from a political perspective.
- How is data managed? What are the encryption processes for data moving into and within the cloud? What procedures are in place for notifying customers of, and dealing with, any data loss or breach?

Finally, you should be comfortable with the supplier, its corporate culture and principles.

simmons+simmons

Key components of a cloud contract

Implementation

In some instances, it will simply be possible to "switch on" the cloud services without any implementation activities. However, where implementation activities are required, this section should cover everything which is needed to get the relationship off to a good start, for example, integration with the customer's existing systems; migration of data, including data protection measures on transfer; and acceptance by the customer.

Operational

Here, it is essential to define accurately the services to be provided and the scope of each party's responsibilities. Suppliers often lack clarity about what they are selling. The availability of the service and the expected performance levels should be dealt with, as should user numbers, storage capacity, and scalability. A customer needs the right to audit the service delivery, both for billing purposes and to monitor the supplier's performance and security arrangements.
Processes for back-up and recovery should also be included. Business continuity and force majeure provisions should work together appropriately to ensure, so far as possible, continuity of service.

Rights and remedies

The customer's remedies if the supplier fails to deliver the services to the agreed standards is probably the most important part of the cloud contract. The supplier will want to cap its liability regardless of the likely loss suffered by the customer if things go wrong. This part of the contract should be drafted with particular care. Service credits are a common solution, but they require careful negotiation if they are to incentivise the supplier while providing meaningful compensation for the customer.

Issues to consider are whether service credits should be capped and whether they are to be the customer's only remedy. At the same time, service credits – or any other form of liquidated damages - must not be so high as to amount to a penalty.

Customers often expect suppliers to give an indemnity in respect of breaches of data protection law, loss or corruption of customer data and claims of intellectual property infringement by third parties.

Exit

Ideally, the contract should provide for a handover period on termination, with the supplier under an obligation to co-operate with the incoming supplier to ensure an orderly transition. The return or cleansing of customer data can be dealt with at this point.

Governing law and jurisdiction

The supplier and customer will often reside in different jurisdictions. It is a good idea to specify the legal system which governs the contract and the jurisdiction for settling any disputes which might arise. However, bear in mind that some aspects of the services may be subject to mandatory local laws in any event.

simmons+simmons

Can financial services firms use the cloud?

Like other businesses, financial institutions are facing increasing demands from customers and shareholders, pressure to drive cost efficiencies, increasing regulatory requirements and tighter rules on data. Cloud solutions may help, provided firms remember that obtaining services from a third party may constitute "outsourcing" for regulatory purposes and will not alter the relevant sector-specific obligations with which they are expected to comply.

The regulators' approach

Financial institutions in the UK are subject to the oversight of the Financial Conduct Authority ("FCA") and, in some cases, the Prudential Regulation Authority ("PRA") as well.

According to the FCA Handbook, an arrangement of any form (i.e., including cloud) between a firm and a service provider by which that service provider performs a process, a service or an activity which would otherwise be undertaken by the firm itself will be an "outsourcing". This is a broad definition and potentially covers a wide range of operational arrangements. Where it applies, the onus is on the firm to ensure its continued compliance.

The approach of the FCA is to ensure that firms correctly identify and manage the risks associated with any outsourcing. According to the FCA's recently-updated guidance, this will involve taking practical account of matters such as legal and regulatory considerations, risk management, international standards, ongoing oversight of the service provider, data security issues, effective access to data and business premises, change management, continuity and business planning, and exit arrangements.

Proposals to outsource functions which are essential to a firm's continuing compliance or financial performance are seen as particularly important and any firm considering such a step must notify the FCA and comply with a number of other conditions.

Dual-regulated firms must notify the PRA of anything of which they would expect to be given reasonable notice and, specifically, should discuss the implications of any proposed cloud solutions with their supervisory contacts at the PRA.

Additionally, as of 30 September 2019, financial institutions will need to review the EBA's revised guidelines on outsourcing and their own outsourcing arrangements, to ensure they are compliant with any new rules that apply specifically to the outsourcing of cloud services.

Embracing cloud

Financial services firms have in many cases been held back by lingering concerns about regulatory compliance, security, the location of data centres and a potential loss of control. Improvements in technology, coupled with a willingness on the part of service providers to adapt, are providing answers. The FCA has also stated that there is "no fundamental reason" why cloud solutions cannot be implemented in a way which complies with their rules. Overall there is no reason why cloud should not be a key component of financial services firms' operational and digital strategies.

Contact us

Alexander Brown
Partner
Information, Communications & Technology
T + 44 207 825 4954
London
E alexander.brown@simmons-simmons.com

Hinal Patel
Partner
Information, Communications & Technology
T + 44 207 825 2080
Bristol
E hinal.patel@simmons-simmons.com

Lawrence Brown
Partner
Information, Communications & Technology
T + 44 207 825 3053
Bristol
E lawrence.brown@simmons-simmons.com

George Morris
Partner
Information, Communications & Technology
T + 44 207 825 4046
London
E george.morris@simmons-simmons.com

James Cotter
Partner
Information, Communications & Technology
T + 44 207 825 3194
London
E james.cotter@simmons-simmons.com

Tom Wheadon
Partner
Information, Communications & Technology
T + 44 207 825 3603
London
E tom.wheadon@simmons-simmons.com

Simmons & Simmons is a leading international law firm with more than 900 legal staff in offices situated in key business and financial centres across Europe, the Middle East, and Asia. We believe it is who we are and how we approach our work that sets us apart from other firms. We set the highest standards for the work we do and pride ourselves on our client focus.

In building our international business, we have created a closely knit and cohesive network of lawyers who seek to balance local business needs with the delivery of a global service. Our current client base includes a significant number of the current FTSE 100 and Fortune Global 500 companies and we advise the world's leading investment banks, many of the world's largest financial conglomerates and more than half of the top 50 European hedge fund managers. We provide services from locations based in Europe, the Middle East and Asia. We work across core practice areas including corporate, dispute resolution, EU, competition & regulatory, employment, pensions & employee benefits, financial markets, intellectual property, projects, real estate, information, communications & technology and tax.

A key commercial advantage for our clients is our focus on specific sectors, including asset management & investment funds; financial institutions; technology, media and telecommunications (TMT); and life sciences. We also focus on the energy and infrastructure market, in particular through our international projects and construction teams.

For additional information on our firm, please visit our website at **simmons-simmons.com.**

© Simmons & Simmons LLP and its licensors. All rights asserted and reserved. This document is for general guidance only. It does not contain definitive advice.

Simmons & Simmons LLP is a limited liability partnership registered in England & Wales with number OC352713 and with its registered office at CityPoint, One Ropemaker Street, London EC2Y 9SS, United Kingdom. It is authorised and regulated by the Solicitors Regulation Authority and its SRA ID number is 533587. The word "partner" refers to a member of Simmons & Simmons LLP or one of its affiliates, or an employee or consultant with equivalent standing and qualifications. A list of members and other partners together with their professional qualifications is available for inspection at the above address.

L_LIVE EMEA1: 45411601v1