



Cloud computing in the public sector

Planning for best practices in next generation IT platforms

April 2011

“Cloud” computing is a term being used in many different ways, many of them seeming to offer the ultimate silver bullet in providing an IT platform. However, many issues currently remain, and it is likely that cloud computing will be many years in maturation and acceptance in the mainstream business and public sector communities.

Governments around the world have been looking at how best to reduce functional redundancy through the concept of “shared services” where different departments share a single source of function. For example, in the UK, a concept for a government cloud (“G-Cloud”) has been proposed to provide the shared services described by Sir Peter Gershon in his 2004 report – but this may have to be revisited under the current government spend reviews.

This report looks at the promise and issues of cloud computing as described today, along with the direction cloud needs to take in order to fulfil on its promise.

Clive Longbottom
Quocirca Ltd
Tel : +44 118 948 3360 ext 200
Email: Clive.Longbottom@Quocirca.com

Bob Tarzey
Quocirca Ltd
Tel: +44 1753 855794
Email: Bob.Tarzey@Quocirca.com

Cloud computing in the public sector

Planning for best practices in next generation IT platforms

The public sector is under increasing pressure to ensure that IT investments both provide flexible support for a rapidly changing world and also do not overly replicate functionality that may be used across central and local departments and groups. Cloud computing looks like it may provide a solution here – but this will only be the case if a measured and realistic approach to implementation and usage is taken.

"Cloud" is not a one size fits all solution

There are many different approaches to cloud computing, and it is important to ensure that the right tool is chosen to meet the requirements.

Technology is reaching a tipping point

Cloud computing will be a fundamental change to how computing services are provided, and the effectiveness of citizen engagement, service provision and cost management will all be impacted by how cloud is implemented and used.

Flexibility provides greater capabilities

The capability for cloud to be dynamic in how it supports the functions running on it means that better usage can be made of the IT assets deployed. This can lead to massive savings on energy bills and space requirements, supporting government green initiatives.

Cost should not be the main factor

An implementation of cloud based on process improvement and effectiveness will lead to cost savings. However, an approach to cloud based on "cost first" may well lead to issues that will be very expensive to fix.

Self-service clouds promote citizen engagement

Enabling the citizen to identify and provision their own services from the cloud is a highly effective means of engaging with them and encouraging use of central and local government services.

"Hybrid cloud" will be the end result

Arguments over "private" and "public" cloud are irrelevant overall - the best systems will combine the best of both worlds to provide the optimum overall solution.

Cloud will be a journey

With standards and overall architectures around cloud still developing, cloud will need to be developed as a long term strategy - not a short term fix.

Conclusions

Although cloud computing is a game changer in both the private and public sectors, it is no silver bullet. Many issues have to be addressed, and existing systems have to be included in the overall architecture. A well-thought out, long-term approach will provide far more benefits to the citizen and the government department or local authority than any quick fix attempt.



The public sector in 2011 and beyond

Historically, public sector IT grew as discrete sets of departmental solutions implemented on an “as needed” basis. Applications, often specifically written to carry out specific tasks, then sat in relative isolation from everything around it. Information such as that identifying individual citizens ended up being replicated in numerous different places and often had input or transcription errors, making an overall view of a citizen difficult or impossible.

In the 1990s, it was fast becoming obvious that public sector technology had to change. More work was outsourced to large outsourcing companies, from basic break/fix support through to major projects for individual departments. However, in many cases, this still led to disparate systems and multiple different places where the same or similar information was being stored. This led to problems not only at the technical level but also in, for example, tracking the increasing numbers of groups and individuals needing to be tracked due to suspicion of involvement in e.g. terrorism or organised crime. Increasingly, a need for joined-up government was being seen – at both the government and the technical level.

In 2004, Sir Peter Gershon published his review on efficiencies across the whole of the UK public sector. In this report, Gershon recommended the introduction of “shared services” – the capability for essential basic services to be built centrally and made available for all those who needed it. For example, single system procurement would enable all government procurement to be centralised, leading to greater strengths in negotiating contracts, in inventory management and in skills usage in such a department.

Although some moves were made towards a shared services environment, the technology was not quite mature enough to provide the flexibility that such a system demanded. However, as standards and approaches have matured, and the price of underlying hardware has steadily fallen, a technical architecture that became known as cloud began to emerge – and looked like it may meet the needs of what Gershon envisaged.

Sir John Suffolk, Government CIO, looked at what cloud could offer, and decided that it could provide a platform for 21st century public service provision. Working from a set of opportunities and constraints, Suffolk came up with a blueprint for a government cloud, or G-Cloud. External companies were encouraged to provide test beds for the G-Cloud to demonstrate what benefits – if any – a cloud environment could provide to the public sector.

Unfortunately, after the financial environment changed and the incoming government embarked on a set of cuts across the public sector to lower borrowing requirements, G-Cloud is under a degree of threat. However, there are costs to not moving forwards, such as the costs of maintaining older systems that may no longer be fit for purpose, in attempting to pull data sources together in a manner that responds to the more dynamic needs of government departments and in maintaining skills in systems that may now be near (or even past) end of life.

Similarly, in the US, President Obama is moving towards a “cloud first” technology approach, where new functionality for the US government will have to be considered in light of cloud computing as a first choice, and can only be implemented in a different manner if there are overriding considerations that count out cloud as a platform. However, with a total federal IT spend in 2010 of \$76b, only \$227m was spent directly on cloud computing – something that will have to be addressed to make cloud a suitable way forward. Departments showing the way include the USDA, where 120,000 employees have been moved to cloud-based email and messaging tools; the GSA, which has moved its citizen portal over to the cloud and New York City, which has identified savings of over \$50m over 5 years by moving its 100,000 employees over to cloud-based applications.

Indeed, as we move beyond 2011, the effectiveness of public sector IT may well define which countries become the “tiger economies” of the post-recession era. Economic constraints forced on the likes of Ireland, Greece and other countries may force through cloud computing as a cheaper means of enacting public sector tasks – and could provide the flexible and open platform required for a cohesive and effective public/private sector interaction and integration. Those countries touched less by the recession may well choose the status quo – and then find that they



are left behind as massively shared platforms in other geographies become a magnet for external inward investment.

Cloud need not be a massive project where everything across a department or group of departments has to be replaced. A sensible, evolutionary approach is possible and would provide extensive benefits to the public sector. Citizens are increasingly demanding that local and central government deal with them in a manner that fits their lifestyle and approach – not dictating how they should deal with those who the general public see as being paid for from their taxes. Failures in managing data, in responding to security threats and in cutting the cost of carrying out simple – or complex – tasks that are invariably blamed on the underlying computer systems are no longer accepted by the public. By narrowing down the numbers of systems being used across the public sector and in sharing information in a more general, yet secure, manner, the public sector would gain efficiency, effectiveness and cost savings and be far more responsive to the citizens that they represent.

Public sector IT in 2011 and beyond can no longer be seen as the home of the big-ticket, long-term project. Benefits have to be more easily realised, have to be easily explained and demonstrated to the public and be aimed at a longer-term strategy for massively flexible government. In Quocirca's view, cloud provides the capabilities for this.

Defining Cloud

Vendors, analysts and the media alike have all been pushing the concept of cloud through 2010. This has led to a plethora of different definitions and cloud approaches being brought to the market – to the confusion of all concerned. For the sake of this document, Quocirca will be using the following general definition of what a cloud platform provides:

- *Cloud computing is a means of providing technology, in the form of resources, applications or functions, in a manner where the resource, application or function is effectively disengaged from the physical IT assets used to provide the actual technology platform.*

In other words, a cloud platform can grow or shrink whatever resources are being provided to meet the needs of a specific workload at any one time through the use of virtualisation and the sharing of the underlying computer, storage and network capabilities.

Throughout this report, Quocirca will be referring to the following types of cloud platforms:

- **Private cloud:**
Private clouds are built on IT assets owned by the organisation using the end output. These assets may be housed in the organisation's own data centre, or housed in an external organisation's data centre facility. The latter means is known as co-location, and IT assets remain the property of the owning organisation, while the overall facility is built, operated and maintained by an external company.
- **Shared private cloud:**
There are two basic concepts to how a shared private cloud can be constructed. One is where parts of multiple private clouds are shared to provide certain functions along a value chain. For example, a government department may want to deal with a few specific large suppliers or with a non-governmental organisation (NGO). By combining specific functionality from the suppliers' own private clouds, information can be exchanged in a secure yet highly standardised manner in order to streamline contract negotiation, as well as inventory and delivery details. The other approach is to provide a central single instance of a cloud that is shared amongst a set of different entities – for example, where public sector bodies need the same functions, such as procurement, HR or vacation planning.
- **Public cloud:**
A public cloud is one where the data centre facility, along with the application or the functionality provided, is all owned by external parties. This may be a complex arrangement – for example, a cloud provider may own the assets that are placed in another organisation's data centre facility (i.e. the cloud provider is



operating an external private cloud for themselves). However, any contractual agreement will be between the end user organisation and the cloud provider. Services in the public cloud can range from the freely available (e.g. Google/Bing Maps) through to commercial offerings (e.g. salesforce.com)

- **Hybrid cloud:**

A hybrid cloud is one where functions are pulled together across a mix of private, shared and public cloud systems. Although this introduces a range of issues, it is the most likely outcome for the majority of organisations and public sector bodies.

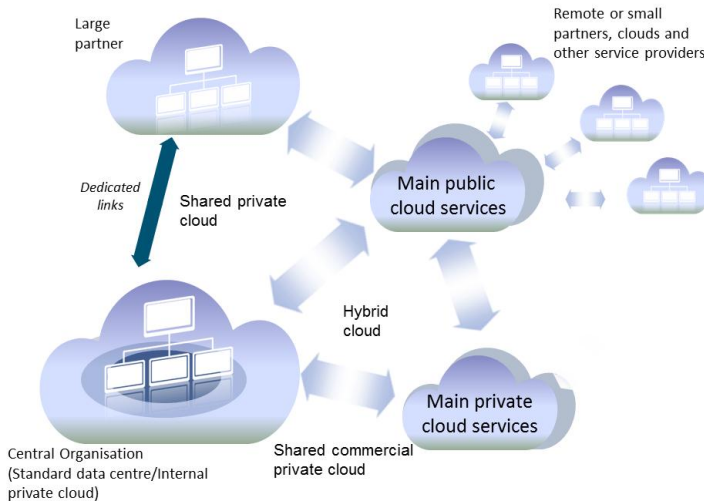


Figure 1

A schematic of how cloud computing is evolving is provided in Figure 1. Many functions will be provided from the “internal private” cloud (i.e. the existing, but modified data centre). Here, existing applications can have functions made available through “wrapping”, enabling these functions to be called and used from elsewhere without having to use the whole of the application for a prescribed process. Incremental new functionality may well be provided from the same data centre but based on highly targeted, small items of coded services that can be called and used as necessary. Other functions may be pulled in from the “extended private” cloud – functions that are run in highly controlled data centres where the hardware and functions are dedicated for specific use by specific organisations. Where a department or authority has to deal with

other departments or authorities, or with NGOs or externals, certain functions may be utilised through the “shared private cloud”. Other functions may best be served by “public” clouds – functions that can be called and used by anyone to carry out specific tasks such as mapping data pulled from the internal cloud onto Google or Bing maps, or in integrating social networking capabilities into functions being used within a more private cloud. The overall approach leads to a “hybrid” cloud platform – across a range of facilities where workloads are spread across data centres controlled by the organisations, where the functions of the data centres are managed on behalf of the organisation and where the data centres’ control is outside of the remit of the organisation completely.

On top of these cloud platforms, there are a number of different cloud services that can be offered by different providers, including:

- **IaaS:**

Infrastructure as a service. Here, the cloud operator provides the managed facility and the IT assets (servers, storage and network). This is then provided on a basis of a virtualised offering such that units of compute power, network bandwidth and storage can be used as a specific workload (provided by the user organisation) requires it. Another version of this is PaaS, or platform as a service. Here, the cloud operator may offer more on top of the hardware, including the base operating system or a stack of capabilities such as a web server, database and run-time environment. However, PaaS will increasingly be used to identify those operators providing a distinct cloud platform, such as Microsoft’s Azure, or dedicated systems such as Amazon EC2, salesforce.com’s Force.com or Google App Engine.

- **SaaS:**

Software as a service. This takes IaaS and PaaS and adds an application or a set of functions on to it. Therefore, IBM’s LotusLive hosted collaboration environment is an example of SaaS, as are the many organisations offering hosted email systems.



- **BPaaS:**
Business process as a service. Here, the cloud operator takes responsibility for a specific function within an organisation and runs it on their platform. Companies such as Concur (managed expense claims and reporting) and ADP (payroll and HR) are good examples of companies that have offered such services for some time.

Other variations on the theme of SaaS can be seen as vendor offers or in the media, including:

- **STaaS, DaaS, DSaaS:**
Storage, data or data storage as a service. The provision of a service that enables data to be stored offsite in an externally managed facility by an external party.
- **CaaS:**
Communication or collaboration as a service. Providers provide hosted voice over IP (VoIP) systems for managed voice calls, or hosted email/collaboration systems.
- **NaaS:**
Network as a service. Essentially a managed connection, often using multi-protocol labelling service (MPLS) to provide service and performance guarantees.
- **DaaS:**
Desktop as a service. The hosting of complete desktop images that are accessed by a remote device. Generally provided as Microsoft Windows desktops, these images will contain all the basic tools required for a user, such as a suite of office applications.

Essentially, as cloud has become more of a discussion point, more and more “aaS” acronyms have emerged. The majority of these will be used by a very few vendors in the market, and will hopefully die out as the market matures. However, the current fad for EaaS, XaaS or *aaS (everything as a service) will mean that users will continue to come up against different terminologies and usages – and Quocirca recommends that any non-standard aaS terms are viewed with the right amount of scepticism.

What does cloud offer the public sector?

Cloud computing brings a different approach to how technology is both provided and consumed. The focus moves from an application to the business process, and flexibility becomes inherent in the overall capabilities of the technology platform. Cloud offers the capabilities to provide shared services between different departments and groups, as Sir Peter Gershon identified as a preferred direction in 2004. For example, a central register of names can still be housed under the electoral roll, but this can also be used as the master database for details in a live environment by other departments, such as housing, health or the UK’s driver and vehicle licensing agency (DVLA). Such sharing of function can lead to cost savings at a basic level – the removal of redundancy in function and data sources means that fewer assets and resources are required to provide such information. At a higher level, however, the benefits of using single sources of information removes issues in data fidelity and in the breakdown in the capability to pull information together in meaningful ways.

For example, data.gov in the US now aggregates 300,000 different data sets in one place. Not only does this help US citizens in finding data at a single source, but also enables local municipalities to access the data on a level footing, without any need to replicate the technical platform, the time or the effort to create similar (yet ultimately different) data sets.

Cloud can also help in dealing with skills shortages and headcount reduction in departments and authorities. For example, a dedicated data centre requires every function to have resources available for installing the requisite hardware and software, in patching and updating the software and in supporting the end users’ usage of the function. Internal private clouds will still need such internal skills, but tools are rapidly becoming available to automate and streamline many of the actions that are required. External private clouds will not require the skills and resources for managing the facility, as these are provided by the facility owner. Public clouds have the



responsibility for managing everything themselves – the department or authority needs only to have enough knowledge as to how best to ensure that the function is used in the most efficient manner and to provide a degree of first level support to the end user.

For the public sector, cloud can also bring in massive benefits when it comes to citizen engagement. For example, the majority of UK, US and other countries' citizens now have access to the internet directly from home, and many more have access via public libraries, other central government offices or public areas such as internet cafes. Many of these citizens are already interacting with each other through cloud-based services such as Facebook, Twitter and YouTube. The citizens are already cloud-savvy; the public sector has an environment that is available for it to drive increased citizen engagement through the use of secure private cloud functions interacting with external commercial and free services where the citizens are already engaged. The big benefit here is reach: attempts to “pull” citizens to government sites in the past have met with poor results. Although the ITU states that the UK had 82.5% (around 51.5 million users) of its population with internet access by June 2010, the society of information technology management, SOCITM, has repeatedly found that the numbers of people using local council web sites remains disappointing, and that overall satisfaction with such sites is poor. The same is found in the US (77.3% penetration, around 240 million users) and across the EU (67.6% penetration, around 338 million users). The main reasons provided are that the sites are poorly laid out, tend to have sections that work in isolation to one another, and that the overall approach appears dated and not up to the levels that the citizen is finding on other sites that they are dealing with. However, cloud-based sites tend to have great reach – for example Facebook has 26 million users in the UK, with 126 million in the US. Many users see Facebook as a relatively central place for them to live their on-line lives – and the public sector needs to understand what the opportunities and risks are of using social networking sites as part of their overall cloud strategies. Alongside this is the continual churn of an individual's favourite social networking site – for example, previous high-riding sites such as Bebo, MySpace and Friends Reunited are hardly used any longer, whereas even the big sites struggle to gain double-figure market share when it comes to actual individual activity at a site. For example, Experian Hitwise figures in 2010 showed that, in the UK, Google UK was the most visited site, with 9.29% of all visits, Facebook was second with 7.04%, YouTube fourth with 2.11% with no other social networking site in the top 10. Therefore, think how difficult it would be to try and recreate the pull of these sites with a private cloud version owned and run by the public sector.

Through the use of external citizen engagement, more citizens can be pulled to the public sector body's site. Here, through using shared services and well integrated cloud systems, the citizen can be led through their issues and provided with a self-service capability for accessing the public services they need. Such an approach provides an effective and low cost public service model, as the citizen no longer needs the costly intervention and redundancy of a public sector employee walking them through the options. This frees up those employees to work with those who benefit the most from them – those who are not internet connected, who are vulnerable or require direct help in identifying what their options are.

The use of external cloud providers also enables a move from a capital expenditure (CapEx) model towards an operational expense (OpEx) model. In many situations, this can be useful, as capital projects tend to be funded from different sources than operational funds. The lack of need to build and maintain a dedicated data centre facility not only offers definite upfront cost savings, but the lack of need to plan for replacement of the facility every 5 or so years also removes a recurring budgeting headache.

Finally, cloud offers the means for the public sector to optimise how it uses its inherent skills and how it collaborates on a more general level. For example, each local authority will have dedicated resources that may be looking at the legal aspects of planning and building, or in dealing with legal cases brought against an authority. Certain aspects of such work may be arcane, and yet it is highly likely that somewhere across the broader public sector, there will be a resource that has domain expertise in that very area. Through the use of cloud-based secure collaboration, one authority or department can more easily identify where the specific skill resides and can use it as necessary – rather than having to fall back on the private sector to provide a service.



Case Study 1 - NATO

Issue: NATO is an organisation consisting of a mix of military and government groups from many different countries and, as such, runs up against issues not only of distributed data sources but also of the need for high security and in dealing with rapidly changing conditions on the ground. With NATO operations continuing around the globe and the nature of its actions continuing to be highly dynamic, existing approaches to providing technical functions have ceased to be fit for function. Dedicated systems for each function need massive redundancy of both platform and function, yet a completely open public cloud solution would not be suitable for operating under the constraints NATO has to work with.

Need: NATO required a technology platform that could rapidly embrace any new technologies, enable systems to be provisioned at very short notice, enable NATO's 28 member nations to share information and services in an open yet secure manner while enabling faster situational awareness and decision making in both battlespace and non-battlespace situations. Such a system has to have military levels of availability, security and resilience while enabling NATO partners to be added and removed from on-going situations rapidly and easily without impacting other partners.

Approach: NATO's Allied Command Transformation (ACT) group was tasked with identifying the best means of utilising emerging information technologies to provide a platform suitable for NATO's needs in the 21st century. Cloud computing was chosen as the preferred technology architecture due to its inherent flexibility, promise of dynamic resource allocation and high utilisation rates and for its capability to operate on a global basis.

Solution: NATO chose IBM as its partner for the creation of the cloud platform. The platform was to be self-contained, built and operated from NATO's Headquarters of the Supreme Allied Commander Transformation (HQ SACT) in Norfolk, Virginia, US. The environment will provide a common operating environment across many mission processes, building in increased security, greater scalability and robustness than the existing decentralised and heterogeneous platforms used across NATO. IBM's existing expertise in cloud and secure military systems meant that NATO was assured of a trusted relationship where both sides could work together to ensure the desired outcome.

Outcome: Such a common platform will enable aggregation and sharing of resources from computer processing power to storage and networks. The NATO cloud will enable the Alliance to deploy IT capabilities more broadly, quickly and cost effectively.



Case Study 2: City of New York

Issue: The City of New York is a massive municipality with diverse needs and citizens. It employs over 300,000 workers covering the needs of 8.2 million inhabitants. Through meeting decentralised needs across an extended period of time, disparate systems had grown up with little interoperability between them, and with redundancy of function and low system utilisation being common.

Need: The city of New York needed to bring together its disparate IT systems across a broad range of functions. It had identified that its existing systems were inefficient at both the CapEx and energy utilisation levels, and that the decision making process across the City was being compromised through siloes of information. A system that could provide a more common platform was identified as a need; one where extra systems could be easily embraced in the future as needs dictated and the platform had proven itself.

Approach: The City of New York implemented a programme for technology modernisation, called CITIServ. Starting from a targeted group of 14 agencies, CITIServ aims to bring together technical capabilities and data so that City employees will be able to carry out their jobs more effectively. The longer term aim is to bring shared services and functional capabilities to all of the City's agencies.

Solution: targeting cross-functional agencies such as help desk, email, shared storage and virtual hosting, CITIServ is working with IBM in order to implement a cloud solution that will provide higher levels of security and availability while optimising hardware utilisation levels and the capability to provision systems in effective timescales. The cloud solution is seen as providing both greater physical and cyber security levels while lowering the City government's carbon footprint. Ultimately, the City aims to consolidate all of its 50 existing data centres onto a cloud platform, not only providing better response to the City's employees, but also providing a single platform from which to better serve the needs of New York's citizens. IBM will continue as a core partner in both the building of the cloud platform and in migrating existing systems to the new platform.

Outcome: The City of New York expects to gain savings of \$100m over a period of 5 years through the implementation of the cloud. Decision making across the City is expected to be streamlined and made more effective, and employees are expected to be able to carry out their jobs more easily. Citizens are also expected to be served more directly through being able to use self-service functions across a broader range of data sets in order to meet their needs.



Even at a basic level, it becomes possible for areas such as public service contact centres to share resources. For example, it may well be that one authority or municipality suffers a major natural disaster, which would normally swamp the capabilities of their front-line contact centre to deal with the number of calls coming through. However, if such services are operated through a cloud-based service, other authorities can help through providing any spare resource to be available to help without the need for them to move to the area where the event has occurred. A prime example here was how cloud computing, combined with the use of social networking, was used in the aftermath of the Haiti earthquake in early 2010. Data was made available from many different sources, resources could be easily pulled together around the globe, rescue and aid workers on the ground could have access to a massive amount of common information and data from Haiti itself could be uploaded immediately to add to the body of information in place. Here, the combination of public sector, non-governmental organisations (NGOs) and private sector groups meant that immediate steps could be taken during the immediate aftermath of the earthquake, and continuing information is still being used now in dealing with the longer term impact, such as the problems of dysentery and cholera during the rains.

At a more prosaic level, cloud also helps the public sector to meet its targets for carbon emissions. A massively shared infrastructure that eliminates redundancy of function and enables the consolidation of physical assets to a much lower number means that less energy is required for powering and cooling the systems, as well as the amount of space required for housing them. As governments struggle to meet the promises made at Kyoto and Copenhagen, yet continue to pass down ad-hoc targets to departments and authorities on how much carbon reduction and cost saving is expected from them, the need for cloud becomes even more apparent. With the capability to invest in more imaginative and innovative low-carbon emission schemes disappearing, the need for highly efficient IT platforms with minimal overlap of function across public sector bodies will increasingly become the only option for carbon footprint cuts in public sector IT.

Cloud and meeting the risk profile of the public sector

By its very nature, the public sector has to be risk-averse. Its expenditure is based around using public money, and the citizens expect to see that such expenditure is reasonable, and that the resulting systems implemented ensure that security of information is a high priority.

Cloud has an unfortunate perception as being inherently insecure. Data has to move out of the owner's direct control to the external data centre's facility – and, if uncontrolled, can be open to hijacking or other compromise. However, suitable controls can be put in place that can minimise data security issues – and in many cases can create an environment that is more secure than was in place with a single internal data centre. For example, ensuring that only the data that needs to be transferred is moved – such as a postcode or zip code for mapping purposes, leaving any personal data such as name or full address – means that the capacity to identify a specific individual becomes impossible. Where personal data does have to be transmitted, making sure that it is encrypted both on the move and at rest means that it is far more difficult for malicious users to capture it and make any sense from it. For interactions with citizens across the cloud into social networking sites, the use of data leak prevention technologies can ensure that information that should not leave the department is captured and prevented from appearing on such sites. This can also include ensuring that language which could be construed as being unfit for purpose can also be prevented from entering the public domain.

There are options available to the public sector. For example, government-owned clouds (such as the UK's proposed G-Cloud, or the discussions the Australian government information management office (AGIMO) has entered into for its cloud strategy) take the essential ownership of the complete system and put it in the hands of the government and/or its trusted suppliers, in the form of systems integrators and service providers. As there is little movement of data outside of the controlled environment, information security is more manageable than if the data were traversing external networks and systems. However, a completely centralised government cloud approach is



unlikely to meet the needs of a multi-level political and governance system and, as such, central, regional and local systems need to be put in place with an overriding umbrella strategy binding them together. The correct touch points between the tightly controlled government clouds and the highly uncontrolled space where the citizens reside also have to be addressed: a stand-alone government cloud strategy will not meet the needs of the citizens, or ultimately the public sector itself. Again, the use of trusted partners who can implement highly controlled and secure cloud platforms that enable audited and managed touch points between these constrained platforms and the more public systems used by the citizens, suppliers and non-governmental organisations may well be the best way forward for the public sector to ensure a long-term, flexible solution.

Cloud issues

Although cloud has a lot going for it, it is not the universal panacea that cures all known ills. In certain commercial areas, such as banking, cloud can introduce latency in how fast information can be provided to employees that can make e.g. trading more difficult. However, few public sector environments outside of defence tend to need such speed of informational provision and, increasingly, the public sector will find that more of its workloads are well suited to a cloud platform. In the meantime, as decisions are made as to which workloads should be moved first to a cloud platform, even with those functions where it is felt that a one-application-per-physical-server approach is still desired due to perceived concerns over possible transactional performance, the more static data surrounding such transactions (such as the claimant's name, address and bank details) can still be separated out and provisioned via a suitable cloud service.

As mentioned above, security is perceived as a major issue, but can be dealt with through a well architected information management approach (see next section).

Cloud computing is still in its early stages and, as such, there is still a high degree of uncertainty and disagreement around how the standards and taxonomies around cloud usage will eventually pan out. Although standards are being worked on, there are many bodies essentially replicating work, with bodies such as the Cloud Infrastructure Forum (CIF), the National Institute of Standards and Technology (NIST), the European Telecommunications Standards Institute (ETSI), the Open Grid Forum (OGF), the Open Cloud Consortium (OCC), the Storage Networking Industry Association (SNIA) and others all having working groups looking at aspects of cloud computing. Ensuring that the overlaps between such groups are minimised and that interoperability between clouds supporting different factions is in place is an area that will continue to stress the cloud model. The key here is to ensure that, as far as possible, de facto standards around cloud are adopted, and that vendor- or group-specific standards are only adopted where such a tactical play can be seen to have massive benefits at a business level for the public sector body.

The robustness of cloud services also has to be taken into account. This is not as simple as it may at first appear, due to the number of variables at play. Certainly, the basic capabilities of a cloud provider need to be checked. Using a massively virtualised environment, uptime should be in excess of 99.5% from an average provider. The use of mirroring across multiple data centres may move this closer to 100% - but at a cost. However, a cloud provider may be able to quote 100% uptime figures to you, but this is only for the facility or group of facilities concerned. Average and trending performance figures also have a part to play but, more to the point, the availability and performance of links to and from the facility can make a cloud service highly available – or not at all. For example, using public networks to access a mission-critical function in an external private cloud may seem like a cheap way to access a known facility with 100% historical uptime. However, a public event, such as a distributed denial of service (DDOS) event, may make the general internet performance so low as to make the usage of the cloud function close to impossible. The use of dedicated network links with managed performance guarantees obviates this problem.

Physical impact also has to be taken into account. Most public sector data centres run on a reasonable level of high availability, with at least mission-critical servers running as clusters or in a failover capacity, such that any failure of a physical asset can be rapidly recovered from. The same needs to be in place for connectivity to mission-critical cloud



services – multiple managed connections need to be in place between the user’s point of access and the point of cloud delivery. In this way, should workmen sever one of the links, automatic failover can be managed to another link so that the user can continue their work.

With external cloud services, contract negotiation can be a major issue. A standard approach of negotiating around a service level agreement may not be the right one and, certainly, negotiating to a price is not an approach that Quocirca would recommend. An outcome-based approach is a far better means of ensuring that cloud provides what you are looking for. Any “big stick” approach will not work – the key is to come up with an agreement that works for the main parties involved – both for the public sector body and the cloud provider. After all, if the cloud provider feels that they have been backed into a lowest cost deal, they will not be inclined to ensure that the best support is always provided, and their margins may be squeezed to the point where any change in underlying conditions (e.g. a large increase in energy prices, the loss of a large customer) could push them out of business – and leave the public sector body needing to identify a rapid means of implementing new equivalent functionality and move data across to it.

In some cases, the public sector body will find that it is dealing with an existing incumbent in the form of a systems integrator or a service provider. Again, Quocirca strongly recommends that the public sector body does not attempt to force a cloud service into an existing framework agreement. Cloud brings in its own needs and issues, and will be best served through the negotiation and agreement of a new set of contracts around the long term implementation, management and evolution of the cloud environment. For example, the contracts need to ensure that flexibility is built in as to how new resources are provisioned – these are not “change requests” as per standard contracts, and the costs associated with such needs should be easily identifiable, and the process for gaining such resources should be rapid and easily carried out. Furthermore, the incumbent should be in a position to provide advice on how to provide the best value from an existing environment. As cloud will not always be the correct answer, existing systems will need to be integrated into what is “clouded”, but this has to be carried out in a manner that provides the best capabilities, through “wrapping” functionality as web services and making them available in the cloud as callable services. Such an approach enables suitable existing software assets to be maintained and extended value obtained from them – but must be reviewed on a regular basis to ensure that such systems have not become a constraint on the overall capabilities of the departments and users using such systems.

The means of paying for a cloud service also needs to be dealt with. Historically, the public sector has either paid on a project basis or on a long-term service contract basis. Cloud is driving a move towards a more subscription style model, where payments are made on a pay as you go (PAYG) basis. However, there are many PAYG business models, such as per user per month, per transaction, per unit of resource being used and so on. Long term, PAYG models should be able to provide the best cost base for the public sector – but are also less predictable than fixed price agreements. Therefore, it is necessary to ensure that the department or authority fully understands the pros and cons of each model and agrees on which fits the strategy of the body in the best manner.

Information management and the cloud

With security being the recurring theme when Quocirca talks with end users around the cloud, it is important to ensure that a suitable information management strategy is in place as a move to cloud computing takes place.

This should start with the use of master data management (MDM). Here, the referential data on an item is taken and is stored in one, relatively small, database. For example, the electoral roll provides a listing of people against addresses, which could provide one master data database. Every time there is a need for any information on a person or a property, that database should be the first point of contact. By aggregating access through this database, security can be managed at a granular level. For example, assume that a health professional requires information on a specific person at an address. The master database can ensure that the name and address match, and can then link through, using a token that is specific to the health professional, to a secondary database that may ask for further validation, which may be aimed at the health professional personally (maybe a one-time challenge



and response password query) or to validate the individual/address match (e.g. through inputting the individual's national insurance number). The health professional can then see any extra information that they have security clearance for, such as further health records held in other subsidiary databases, or details of when the last care worker visit was to the address. Another example may well be for an emergency services worker attending an accident. They have identified the name of a casualty, and have part of an address. By accessing the master database, they can be given all matching records – something that may not be offered to a health professional, as this may be outside the security level deemed necessary for their work. Once the emergency service worker has identified the casualty, a paramedic may be able to then access full medical history, whereas a police officer can gain telephone details through cloud services from a commercial entity so that they can get in touch with relatives, and details can be input by other police officers on the accident itself, including detailed maps based on using publicly available mapping software driven through the use of GPS, prevailing weather details available from weather sites and so on.

A local authority or municipality will have mapping details on all public services (water, drainage, gas, electricity, communications, etc.) that will generally be applied against an in-house geographic information system (GIS), such as PBBi's MapInfo. While it may be tempting for such a package to be shared amongst the greater public sector for basic geographic services, the use of Google or Bing maps is generally more than enough – and is provided on a free basis. Information security can be maintained by only sending the very basic data needed to identify what is required; any additional collating of data that adds personal details or information of external value can be done through integration of the public cloud function into the process such that all personal data remains within the secured environment.

The next step is to secure any data on the move and at rest that may have perceived value outside of the public sector department. Here, encryption is the preferred option, but obviously cannot be used easily where public cloud services are going to be used, unless the public cloud also supports the form of encryption to be used.

Data leak prevention can be used to ensure that information that should not leave specified areas stays within them. Here, information is examined as it crosses boundaries, and word patterns combined with heuristic algorithms that can identify close or associated patterns of words, similar words and sound-alikes means that end users can be trusted through accidental and malicious data leakages being prevented.

Next comes individual and role identification. With the public sector being so all-encompassing, basic rules cannot easily be applied. Therefore, the capability to ensure that shared services are only available to those that are authorised to use them becomes very important. A massively centralised system runs the risk of being compromised, in which case all dependent systems will also be compromised. Again, MDM helps here. A centralised database containing the names and roles of all those who may have access to the public sector cloud services can be created. Even if this is compromised, it is no major problem, as it can easily be replaced. Under this can be any number of dependent databases containing security details that provide access to associated cloud services and functions, but only being referenced through, for example, a hashed security token held in the master database and the main slave. Individual tokens can then be allocated to provide access through to specific functions. Any security breach only impacts one specific area, which can be dealt with in isolation to the others, enabling work to continue across the broader cloud spectrum. The use of federated identity management provides additional security, with individuals carrying a single identity with them across multiple systems, whether these be the remaining physical systems or the new private or shared cloud platforms.

Then comes the physical security of the cloud facilities that you will be dealing with. In Quocirca's view, any facility where data security is an issue should be able to demonstrate security policies and procedures to e.g. ISO 27001, along with being able to demonstrate how only named people will have access to your equipment and be able to access command line interfaces and so on. Admin and other trusted user passwords should be demonstrably controlled, with no sharing allowed. The facility itself should have anti-ram bollards, have physical security including CCTV, secure electronic lock and possibly biometric entry systems, along with policies like not allowing two people entering through any controlled door at the same time. Indeed, governments around the world often dictate that certain security measures be adhered to; for example, the US mandates OMB M-06-16 and FISMA in how departments have to manage security and that vendors have to be able to demonstrate compliance, while the UK is



currently putting in place a new security mandate around the proposed public sector network (PSN) that would provide the connectivity around any future government cloud strategies.

Again, Quocirca believes that the facility itself should have dedicated rooms for co-locational equipment, should have real floor-to-ceiling (i.e. not raised floor to dropped ceiling) cages, should ensure that any administration terminals are not visible from outside the room, and should use a means of identifying if there is someone within an area.

On top of this, there are other aspects of data security that should be in place, such as adequate fire suppression, flood avoidance and recovery plans and capabilities, adequate back-up power along with redundant power distribution as well as multiple internet connections. Also, data should be capable of being mirrored and securely backed up and restored – even if this is at an additional cost as a value-add service.

Overall, the security of the majority of managed cloud facilities (and even the majority of public cloud services) will exceed that of the general in-house data centre outside of the defence and security services. It has to be remembered that providing a suitable environment defines whether a cloud provider survives or not, and that security is a core part of this strategy. The majority of the skills involved in security have been moving to the large providers – it has become increasingly difficult for private companies or the public sector to attract and keep the skills required to create a complete, comprehensive secure environment in place.

Putting in place a cloud strategy

Implementing cloud should be seen as a long-term journey, not as a one-project destination. Several areas need to be considered before starting the journey, and then other areas can be addressed as the cloud concept matures and capabilities become apparent.

Quocirca recommends the following stages in starting the cloud journey:

- A full analysis of what you already have at an application level
- Identify which core processes could best benefit from being cloud facilitated
- Prioritisation of which applications need replacement in the immediate, short- and mid-term basis
- An analysis of what functions each application provides
- Identification of where functionality is being replicated
- Choice of which functions are key to continuing processes
- Identification of what services may already be available through shared services with other public service bodies and trusted partners
- Identification of alternative external cloud-based services
- Choice of whether to use internal services (dedicated or shared) or external (commercial or free) cloud services
- “Wrapping” of internal services using web services to make them cloud-capable
- Firm up information security policies and implement suitable technology internally
- Move towards an internal cloud architecture
- Integrate external cloud functions as required to provide support for the department or authority’s processes
- As new functions are required, analyse whether it is more effective to bring them in from the public cloud, whether they should be provisioned in the external private cloud or in the internal private cloud



Conclusions

Cloud computing is both an evolution of current thinking, taking historical concepts such as on-demand computing, grid computing and virtualisation to another level, and a revolution in the provision of function to the public sector, the end user employee and the citizen. The use of shared services enabled through private clouds, combined with the use of public cloud services, where appropriate, can lead to far more effective citizen services, while driving down costs and the carbon footprint of public sector IT.

Cloud is not the ultimate answer to everything, and certain functions may still need to be dedicated to specific hardware, due to specific needs, need to prioritise other workloads as being better suited to a cloud environment or pure perception as to where a workload is best suited at any one specific time. However, peripheral functions around these workloads may be offloaded to the cloud, so freeing up resources to deal with any growth in the core workload as time goes on.

Although security is perceived as a major issue within cloud computing, Quocirca does not believe that it need be. The basic levels of security within the cloud already exceed the security of the majority of private data centres and, when combined with an appropriate information management strategy, can be managed for optimum security.

The current view around the globe for public sector is focused on cost savings. While this will, in many cases, modify or postpone cloud strategies and implementations, for those public sector groups who approach cloud in the right manner, a cloud environment should provide a cost-effective platform where essential core services can be easily shared, where information is managed in a far more centralised and consistent manner and where changes to needs, driven through central government or the citizen, can be easily embraced. Cloud computing in the public sector is not an “if” – and should not even be a “when”. A move to cloud – even if it is carried out in a manner where only certain workloads are moved to start off with – can provide direct cost savings while providing a far more optimised and effective service to employees, partners and citizens.

That the very success of a nation can depend on how well its central public services are run cannot be undervalued. That the current state of the public sector around the globe is being affected by the aftermath of recession and by geopolitical upheaval may mean that certain countries are forced into adopting a more low-cost, flexible platform and find that cloud offers this. If adopted on the right basis, these countries could well become the best-positioned to make the most of the new world beyond the current time. For those governments taking an approach of only sweating existing IT assets, this may prove to be far too short sighted. Being left with systems that are unfit for purpose post-recession will hold back these governments, and may well reduce GDP as inward investment goes to those countries who can demonstrate a more flexible approach to how it deals with other government and non-government bodies. The key has to be to develop a strategy for cloud adoption now, starting with those workloads where the biggest savings can be identified and where the greatest effectiveness gains can be seen. As cost savings are accrued, part of these can be applied to moving more workloads to the cloud and further improving efficiency and effectiveness.



About IBM

IBM has helped thousands of clients adopt cloud models and manages millions of cloud-based transactions every day. IBM assists clients in areas as diverse as banking, communications, healthcare and government to build their own clouds or securely tap into IBM cloud-based business and infrastructure services. IBM is unique in bringing together key cloud technologies, deep process knowledge, a broad portfolio of cloud solutions, and a network of global delivery centres. For more information about IBM cloud solutions, visit www.ibm.com/smartcloud



REPORT NOTE:

This report has been written independently by Quocirca Ltd to provide an overview of the issues facing organisations seeking to maximise the effectiveness of today's dynamic workforce.

The report draws on Quocirca's extensive knowledge of the technology and business arenas, and provides advice on the approach that organisations should take to create a more effective and efficient environment for future growth.

About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first-hand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to provide advice on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, Microsoft, IBM, O2, T-Mobile, HP, Xerox, EMC, Symantec and Cisco, along with other large and medium-sized vendors, service providers and more specialist firms.

Details of Quocirca's work and the services it offers can be found at <http://www.quocirca.com>