Brought to you by Socitm Ltd | Reference: 21004

Report

Cloud computing

What public sector CIOs (and their suppliers) need to know

February 2021

Socitm inform

Table of contents

Introduction

It would be easy to assume that there is nothing new about cloud computing. After all, it has been around for nearly 20 years. Socitm's first briefing on cloud, 'Heading into the Cloud' is still relevant today and was published in December 2010.

We still read, almost on a daily basis, articles telling us about the benefits and value of cloud solutions for business and IT leaders alike. Meanwhile, the cloud computing supply side is maturing, with suppliers now offering edge computing,[1] pay-as-you-go charging by the second, and a consolidation of Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

Yet the public sector continues to be criticised that its take-up of cloud computing is too slow, resulting in a retention of inefficient and outdated IT models and services. The cause, we are told, is the public sector's resistance to change, over complex and immoveable legacy technology and a desire to retain control and to run services 'on-premise'.

However, the true picture is not so simple. Cloud sellers often oversell the benefits of cloud or, at the very least, misunderstand the risks, costs and challenges of cloud adoption in a public sector context. They see the value in the narrow scope of their cloud solution but not always embracing the complexity of cloud adoption across a public sector organisation, such as a local council. Notably, cloud is often sold as a 'product' rather than a 'service', which can misrepresent true costs over time, especially if a public service is not skilled in cloud provisioning and cost control.

It is unsurprising then, that parts of the public sector have acquired cloud solutions on a piecemeal basis in response to either internal pressure or supplier mandated change, creating potential future legacy problems. A lack of strong governance, unclear cloud adoption policies and weak supplier due diligence checks, or even supplier-led SLAs can be problematic, especially where a cloud offering is a poorly architected version of a previously strong on-premise solution.

Public sector leaders are also not just worried about cloud security (the single biggest reported inhibitor in most surveys of cloud adoption). They have a wide range of compliance issues to consider in a migration to cloud computing, including data management, disaster recovery, data location, support and avoiding supplier lock-in. Many CIOs still report that they face internal challenges generated by shifting capital IT projects to revenue-funded 'pay-as-you-go' cloud services.

This report offers a practical guide for the public sector CIO and other public service business leaders into the realities of cloud challenges and opportunities of today. It lays out the issues and opportunities raised by cloud computing in the public sector and how best they can be tackled.

Our advice is timely because, despite its maturity, cloud adoption in the public sector is on the cusp of major growth, partly to support more flexible and resilient business models in a post-Covid world, and partly to exploit emerging technologies such as 'low code' application development, AI and IoT.

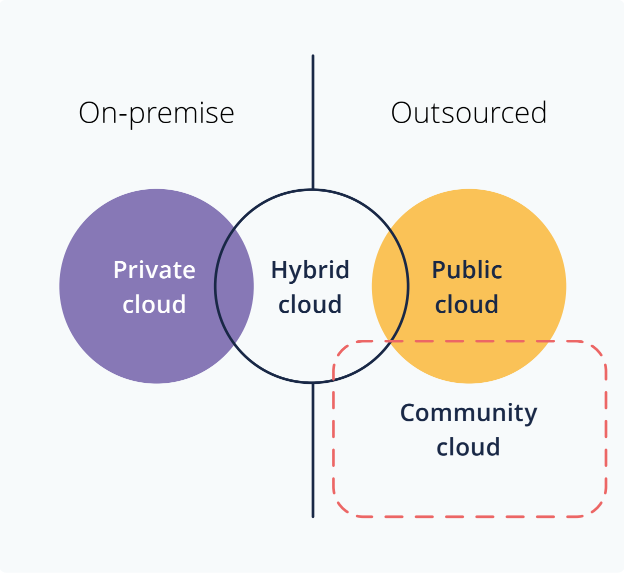
1. Cloud types in use

If you are reading this, you may already be well versed in the differences between cloud models. The general view is that there are only two models for delivering cloud computing: public and private (or a 'hybrid' of the two).

In simple terms, a 'public cloud' is one that is used by many clients, publicly available and run externally on a hosted, 'Software as a Service' (SaaS) platform.

A 'private cloud' is a similar SaaS model, in terms of the way it works and the benefits it offers but is typically run in a local 'on-premise' data centre.

A 'hybrid cloud' model simply reflects the fact that most organisations use a mix of both public and private cloud services. A 'community cloud' is just a special case of an infrastructure accessible to a specific community, which might include a specifically designed secured shared service platform.



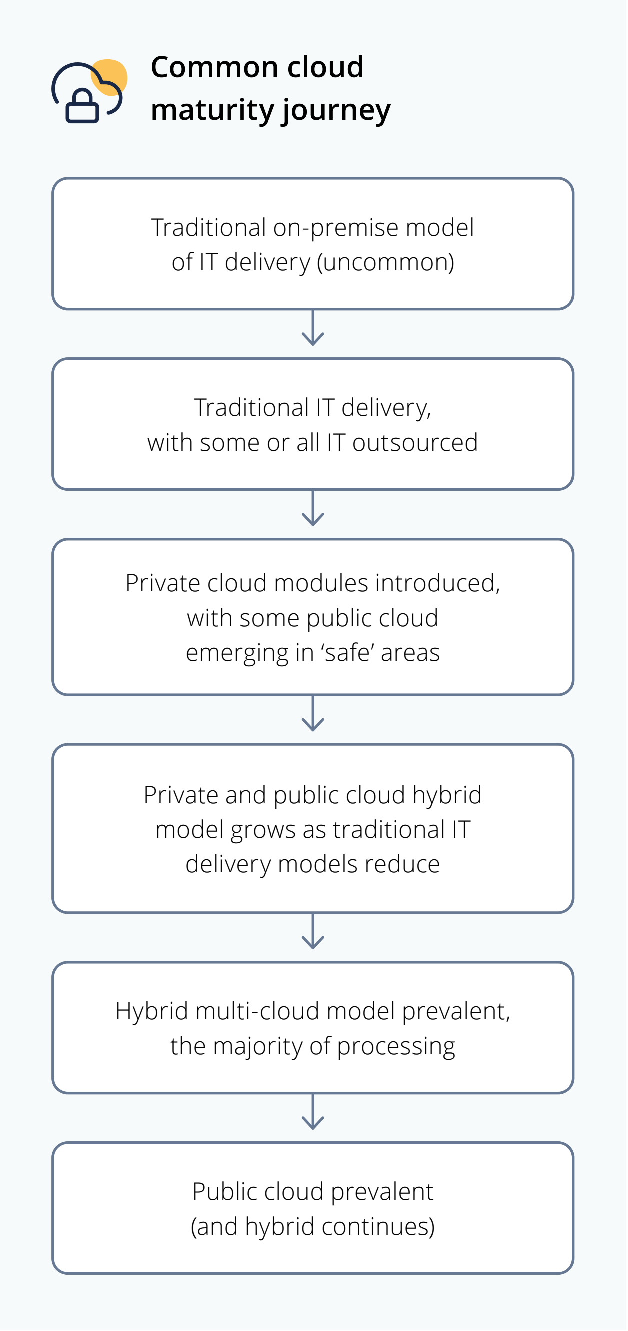
A variety of cloud solutions (cloud service provider services) may be delivered from any one of these models. A CIO needs to ensure that the differences are understood, in order to guide decisions about how new Cloud Service Providers (CSPs) and their products and services are selected as part of a cloud 'multiverse'.

Type	Description	Practical advice for the CIO
Hosted cloud platforms	These are the mainstay of many types of cloud solutions, offering basic cloud infrastructure as a service (IaaS). They include the basic cloud platforms offered by hosted web services and also the giants such as AWS from Amazon and Azure from Microsoft.	It can be assumed that the recognised brands are safe, secure and resilient. However, care is needed in how sensitive data is tracked and shared, where data is located and processed, and that pricing structures of cloud services are understood as workloads grow or shrink. But note that some cloud suppliers offer poorly architected cloud options.
'Line of business' cloud services	These are the services that used to be on-premise and now mostly or only in the cloud. Many specialist applications fall into this category, such as ERP software from the big vendors such as Oracle or SAP or applications service specific areas such as social care, library software, planning – the list is huge. Some are generic but many are tailored and proprietary.	It is easy to end up with a patchwork of cloud systems as all application providers move to cloud provision. A firm framework of policies, security protocols and standards can help, avoiding suppliers with highly inflexible or proprietary standards (especially for data). Where possible, use a public cloud version, with minimal customisation, or containerise a proprietary service.

Type	Description	Practical advice for the CIO
'Low code'	A number of vendors offer cloud-based solutions for low code or no code development, such as IEG4.	These are growing in popularity and can usually run on-premise or on recognised cloud platforms. However, check for common and open standards for data.
Consumer apps	Many consumer apps find their way into a corporate environment and are all cloud based (typically though not exclusively public cloud). Examples include a range of collaboration tools such as WhatsApp.	It is easy to dismiss these as not suitable in a corporate environment, but this can be a mistake. They are popular, easy to use and recognised – banning use entirely may not serve the CIO well. What is important is how they are used and ensuring that the way data is accessed and shared does not compromise security or data protection. The key issue here is user education.
Universal services	The major email platforms, such as O365 or Google fall into this category – they are now so entrenched that many organisations have little choice but to adopt them.	Determining a broad family of IT products is a sensible step for the CIO but not everything has to be from the 'same stable'. The ability to use specialist tools alongside the core systems can reduce cost and improve functionality. Customisation and tailoring of these tools is often possible, perhaps deciding which functions to turn on, the appearance of the desktop and even embedding external utilities such as secure email transfer into the service. However, care is needed to avoid creating a bespoke service that is expensive or difficult to integrate and support.
'Home grown'	These include home developed solutions and a wide range of tools, customised to work on or off premise.	Where in the past the CIO is expected to resist any local development work in favour of off the shelf solutions and packages, in the public sector at least this has proved somewhat problematic. The market is such that many of the specialist solutions from the private sector have proved to be less than adequate, or more expensive than hoped. Many public service organisations are therefore beginning to turn to development work, even in partnership to share services. However, care needs to be taken to optimise performance and security, to avoid creating future legacy overheads, and to maintain the necessary level of skills and resources for support and development.
'Cloud native'	'Cloud-native' applications are typically a collection of loosely coupled microservices, designed to provide a consistent development and automated experience across private, public, and hybrid clouds. Typically, open source, public cloud-based, but containerised, operating as 'Lego pieces' that can be connected to provide a variety of services.	This is a way to ensure new applications (and repurposed legacy applications) are specifically designed for the cloud from day one. They can be deployed and fixed faster, have a more fluid architecture, and can be placed and moved through different environments easily. But the CIO will need to ensure that their team has mature methods for development and optimisation, as well as integration skills, before embarking on a wholesale replacement of legacy applications

Importantly, the CIO needs to see cloud as a move away from inflexible and old-fashioned IT outsourcing contracts, whilst recognising that managing a multi-supplier environment will require a structured approach and a reskilling of internal staff to oversee a new service model, often referred to as service integrating and management (SIAM).

Typically, as a public service organisation matures in its approach to cloud, it follows a common path, as illustrated below:



Common cloud maturity journey

Traditional on-premise model of IT delivery (uncommon)

Traditional IT delivery, with some or all IT outsourced

Private cloud modules introduced, with some public cloud emerging in 'safe' areas

Private and public cloud hybrid model grows as traditional IT delivery models reduce

Hybrid multi-cloud model prevalent, the majority of processing

Public cloud prevalent (and hybrid continues)

2. Realising the benefits

A widespread trend is to move data processing to cloud computing platforms, whether private cloud 'on-premise', public cloud or a hybrid mix. Cloud has become 'business as usual'. Yet at the same time, simply accumulating cloud services without careful planning can be a problem, given their fundamental impact on IT strategy and infrastructure, and on business behaviour.

As cloud adoption accelerates to provide the main platform for new technologies, such as IoT and AI, public services need to review their IT policies, practices and strategies to ensure that 'cloud' is not just a 'business as usual bolt-on' to traditional and legacy IT functions. Resetting has become more pressing as a result of Covid-19; experience suggests that cloud offers the best way to support remote and flexible working for staff, partners and for the public, especially if it is not 'on-premise' but based on public cloud platforms.

For many public service organisations, cloud also offers a welcome alternative to traditional IT outsourcing, which has often failed to deliver promised flexibility, innovation or IT cost savings.

With a heavy supplier emphasis on the theoretical benefits of cloud models, there is often a need for advice on how to realise the benefits. This should not be surprising – it is difficult to do - and it falls to the in-house team to deliver, once the supplier has sold the goods. Consider, for example, the promised savings in costs from moving to a cloud model, both in IT operation and the business more generally.

In 2020 Accenture undertook a global survey of IT executives[2] to investigate the reality of cloud benefits, reporting that nearly two-thirds of companies report they have not achieved expected cloud outcomes and value. They also found the main barriers to achieving the desired results lay in security and compliance risk.

Cloud benefits

Resilience

In addition to the potential security benefits, disaster recovery can be stronger from a reputable cloud platform simply because of the investment, testing, redundancy and critical business interests at stake. Data is typically available at any time and any location connected to the internet, and cloud can also be used as a temporary basis for testing or backup.

Security

Whilst this remains the biggest concern of the CIO in cloud adoption, it is also one of the advantages of cloud adoption. Reputable cloud providers ensure security is their highest priority, and can invest heavily in order to protect their reputation and deliver best practice.

Savings

There are significant potential cost savings from cloud. In IT these will be in data storage, reduced capital investment, productivity of staff and reduced processing redundancy. A 'pay-as-you-go' model will also allow faster response to changing IT demands and is typically better than traditional outsourcing. But many savings are outside IT and in the wider business ROI. This typically requires a commitment to business change in new delivery methods.

Collaboration

Every service organisation has a growing need to collaborate. Sharing data, information and systems is much easier in a cloud-hosted environment, which arguably also makes accessibility and data sharing easier and simpler. Many new collaboration platforms and tools are only available in a cloud environment.

Flexibility

Every workforce in every organisation has become more agile in recent years, and much more so recently as a result of Covid-19. The ability to work anywhere at any time is, for example, enhanced through the cloud with easier access to corporate data from anywhere, by anyone, with any device. A cloud-based service can adapt to changing demands more rapidly and at a lower cost, with ready scalability.

Innovation

A cloud platform can, in theory at least, give access to a range of innovative solutions that might be difficult to procure, to develop or to afford and run on-premise. This also includes a range of automated updates and patching, shared with many other clients. Roll-out is faster and development controlled.

Sustainability

This is an increasingly important topic for IT delivery, and a significant volume of redundant capacity or inefficient processing – which is often unavoidable on-premise – carries a heavy green overhead.

Careful planning, change management and pragmatism are needed to realise the benefits. In particular, assessing the cost of change can be a challenge – recognising that there is a cost, but not using this as an excuse to maintain the status quo by overstating it, and bearing in mind the on-going costs of not changing.

Moreover, a simplistic view of cost savings from cloud typically needs to be reassessed against the challenges in delivery:

Lower costs in IT

This is one of the biggest promised benefits of cloud. But, in practice, the savings in IT may be more modest than hoped since suppliers tend to sell the maximum potential. Also, some of the biggest promised value lies in using cloud to drive IT productivity i.e. allowing scarce IT resources to be redirected to other more critical work to support digital transformation, which can be hard to measure and track.

The business case for cloud services therefore needs to be clear as to where the IT savings actually lie and how they can be harvested (not just reinvested). Examples include:

- IT staff costs may reduce, but unless there is a wholescale move away from on-premise infrastructure, they may be modest or hard to realise by reducing IT headcount.
- A major shift to cloud can also take away a significant management overhead of planning and delivering operating system and platform upgrades which often create business downtime.
- Hardware costs may reduce if substantial processing takes place in the cloud, provided it is possible to retire parts of the infrastructure (rather than increasing on-site redundancy).
- Data storage cost will almost certainly reduce – cloud storage is much cheaper than on-premise due to economies of scale. But data storage is low cost already, so savings may lie in the future growth of data volumes rather than current estate and may prove to be modest.
- Software licence costs could reduce, especially if a major and over-priced contract for on-premise software can be replaced with a simple 'Pay As You Go' cloud alternative. Equally, some cloud models are becoming more expensive in licensing than previously, so care is needed.

Of course, shutting down an on-premise data centre entirely in a move to public cloud could offer substantial savings, although 'sunk costs' that cannot be retrieved will need to be considered. Moving from unpredictable and regular capital investments in IT to a more defined monthly revenue spend could be attractive. Yet, even then, there are likely to be new costs in other areas; network, support and security management overheads may increase and need to be offset against savings.

Lower costs in services

Growing maturity in both technological and business understanding of cloud models means that most organisations now rightly see cloud as a way of saving money beyond the IT department.

However, much of this potential efficiency lies in being able to deliver complex business change that drives productivity improvement. This can be hard to measure, let alone realise, because it depends on services being redesigned to exploit a new cloud solution, for example to support new flexible or collaborative working.

If a cloud service allows greater flexible working and sharing, will the service respond by reducing staff and travel costs, adopting new ways of working, with fewer management overheads and lighter governance models? In particular, administrative, corporate and buildings costs could be reduced.

A business case for a new cloud solution should show how business value improvement will be measured and extracted, and tangible benefits realised. This includes identifying and managing dependencies, especially since that is where the biggest yields are to be found from cloud adoption.

Note also that the benefits from cloud adoption can often be accrued across services – in other words, where similar areas join together to use a single cloud solution, consolidating and standardising process and practice, retiring any duplicate IT and business processes. This in turn requires a non-silo approach to IT adoption, with services agreeing to collaborate and, if necessary, to compromise on long-standing ways of working, even adopting sub-optimal cloud services for wider corporate benefits.

Imagine the challenge and potential benefits of social care and health services sharing a single cloud architecture with community and public across the whole of the UK.

The CIO needs to work closely with business colleagues and the CFO to translate the practical opportunities of cloud into a deliverable and realistic business case, recognising the risks alongside the benefits, including cashable savings and non-cashable but measurable value improvements, both in IT and more widely across the organisation.

> *"There is still a strong business case to own your own on-premise infrastructure... and adopt cloud services where it makes sense.*
>
> *A modern on-premises hyper converged infrastructure can be as agile and cost-effective as the public cloud, especially when you extrapolate the costs over five years or beyond.*
>
> *It makes sense to sweat assets beyond the initial expected lifespan and it is still early days in understanding the long-term modelling of cloud costs."*
>
> **Tony Doyle**
> Head of ICT services, Blackpool Council

This work should be part of the wider corporate digital planning as much as IT strategy, ensuring that an objective and holistic assessment can be made of cloud adoption, whether public, private or hybrid.

Some of the common myths about cloud are set out in Appendix A.

3. Building a business case for cloud

The business case for cloud computing extends beyond simple consideration of cost savings. Being able to avoid the traditional cycle of IT capital investment, often unplanned and unpredictable, and generated by growing demand and outdated infrastructure, will appeal to CIO and CFO alike.

Where the move to cloud operating is carefully planned and integrated into IT strategy, it can also take away significant management overhead in IT planning and upgrades. However, this depends on having a mature approach to cloud, including IT supplier management, IT integration mapping, data asset control, change control and procurement due diligence.

Addressing these issues will reduce both planned and unplanned business downtime, and can offer significant, positive cost benefits.

There is also value in reducing the level of redundant IT processing and management capacity required to address fluctuating demand levels and that cloud services are designed to absorb, for example:

- Reduced demand for processing weekends and holiday periods
- Increased demand for systems testing, dual running, and transition
- Accommodating backup and disaster recovery testing.

Cloud platform suppliers can also deliver significant economies of scale, compared with buying infrastructure and hardware on premise. This can include cheaper processing and data storage, and much faster access to resources when there is a need to rapidly grow a service.

But the greatest benefits from cloud computing lie in creating business flexibility, such as supporting a more agile and remote workforce, as has been evident during the Covid-19 pandemic.

One factor to tackle early in developing a business case will be the inevitable move from 'capital' to 'revenue' expenditure. Many CIOs in the public sector report difficulties in 'selling' this approach internally at a time when revenue budgets are under immense pressure. Yet the public sector has to rebalance its revenue expenditure towards digital and IT investment as more services move to becoming primarily online and driven by greater collaboration, harnessing relevant technologies and data sharing.

An early discussion with the CFO is essential, since there will typically be knock-on effects across other budget lines in the organisation. It is also important for CIOs to be able to explain the benefits and the challenges, since in some public services there is a growing view from the top of the organisation that the only option is cloud, and the business case just has to fit.

> *"CIO's need help to address a common CEO view that Cloud is the only way and if we don't adopt it now we are behind the times"*
>
> **Anon**
> CIO in a UK council

Typically, there will also be transitional costs in moving to a cloud model, while data and systems are tested, and implementation rolled out. Decommissioning legacy applications may also take time, and some IT costs may even increase, including in areas such as networking infrastructure and resilience, and security architecture and service support.

More importantly still, the migration costs need to be considered in the business case; there will be complex areas around data migration, testing, integration and benefits realisation activity that will need to be resourced.

4. Not attempting everything at once

In the pressure to exploit cloud value, CIOs also need to avoid taking on too much at once. Too many concurrent cloud implementation and transformation projects can be confusing and challenging in terms of governance, supplier management and change management.

For the CIO this is not a cloud-specific problem but a typical IT project challenge. There are times when the CIO and their teams are inundated with project requests, for example:

- At the start of a new budget cycle to catch up on a development backlog
- In response to a major change (such as Covid-19 and the need for mobile working)

> *"Cloud can reduce cost, effort and risk across the public sector, as well as responding to the need for greater flexibility in services. But this depends on change, both in IT and in citizen service redesign, if the full potential of cloud is to be realised in the sector. It is more than buying the right cloud service."*
>
> **Steve Lawrence**
> Chief growth officer, UKCloud

- To accelerate a digital programme held back by legacy IT constraints
- With a change in leadership (political or executive) and priorities.

However, with the adoption of cloud services this pressure can be magnified by consultants and suppliers, especially when it is said that the public sector is 'too slow' to adopt cloud and to realise its benefits.

Sometimes there is no choice but to manage a large portfolio of projects, but a transparent and inclusive prioritisation mechanism can still help to order them as they emerge from different parts of the organisation.

For the CIO doing the pre-planning with a clear set of generic cloud requirements and cloud adoption policies, this is also the opportunity to manage internal expectations for new cloud services.

Understandably, the view of the internal 'line of business' client manager, seeking to adopt a proposed cloud offering for their services, will be influenced by persuasive supplier marketing. This can put the CIO on the back foot, having to explain the risks and downsides of what appears superficially to be a valuable and innovative cloud offering.

Many CIOs describe the intense pressure from some of their business colleagues to adopt a cloud solution because of the specific business function it brings. These colleagues are inevitably less interested in hearing about IT downsides or risks that may exist (or at least need to be checked out before deciding on a tender or purchase).

Assessing the risks, costs and opportunities of a proposed cloud service against a set of pre-defined and agreed corporate criteria for cloud adoption, will help the CIO not to appear to be a 'blocker' or a pessimist, or holding the business back from innovative improvements. At the same time, the CIO cannot be overly risk averse, seeking to eliminate or just to mitigate every known and unknown cloud and data risk.

Above all, the value from a cloud migration lies as much in being able to change business models as in reducing costs or increasing flexibility in IT operation.

If this is not acknowledged and planned, for example in measurable service productivity improvement, then the cloud service should be postponed.

Prioritisation of cloud projects

1. Business critical

- Essential for service continuity in an area which has direct, immediate and positive impact on risk and public well-being
- A core part of a corporate digital programme, without which a wider set of changes cannot start

2. High importance

- Will deliver immediate savings at scale, with a strong ROI and definable risk profile
- The project is essential for business improvement in at least one area across the organisation, and is a high digital priority

3. Business improvement

- Everything else! All the worthy programmes and projects with savings, service benefits and a pressing business case:

  a. Small and quick wins that will unblock and empower change

  b. Significant savings and measurable service benefits aligned to corporate outcomes

  c. Less tangible benefits that are considered 'important', perhaps in specific service areas

'Cloud first'

The government introduced a mandated 'Cloud First' policy in 2013 for all technology decisions.[3] This meant when procuring new or existing services, public sector organisations must consider and fully evaluate potential cloud solutions as a preferred option before considering any other solution. 'Cloud First' also meant 'public cloud', rather than a community, hybrid or private deployment model. This was mandatory for central government and recommended strongly elsewhere. Numerous councils have today adopted a 'cloud first' policy – prioritising cloud solutions over more traditional acquisitions or developing solutions.

In practice, this is often interpreted as 'cloud preferred', which could include development of on-premise, private cloud models, as well as more traditional alternatives. Previous research in 2018 by Socitm with Eduserv (now Jisc), concluded that mandating a 'cloud first' policy without a wider assessment of local circumstances could be a mistake, since it would focus too much on the theoretical efficiency promises and less on risk and other factors such as digital maturity.[4]

That research also identified that many councils still had some way to go to understand how cloud can play a role in modernising services, and that maturity was often lacking in responding to the risks of cloud corporately, including security and data governance. But it also concurred with the GDS view of the wider potential of cloud for the public sector. This is especially true for smaller organisations such as district councils that can, through cloud, access technology that previously would have been too big, expensive, or complex – particularly if they collaborate and also use G-Cloud.

5. Managing cloud risks

For many CIOs, the main risks of cloud computing are seen to be in maintaining resilience, and control of the technology environment, security and data management. Yet these fears can be misplaced, since cloud also promises to reduce risks in each of these areas, if service selection and adoption are planned with care.

At the same time, outsourcing workload to the cloud does not outsource responsibility for risk. With some loss of technology control inevitable, CIOs need to ensure they have sufficient supplier monitoring and security reporting to be aware of the changing risk landscape.

In addition, there is a risk in every organisation of unauthorised use of apps and cloud services because accessing them is so easy, without IT consent or even visibility. Effective corporate IT governance can mitigate this risk, with all parts of the organisation being accountable for their actions when accessing or commissioning cloud services.

> *"Many local authorities take a 'cloud where appropriate' approach. Move to cloud where it makes sense. e.g. best in breed product or transformational change such as Microsoft Teams versus traditional telephony."*
>
> **Kurt Frary**
> Deputy director of IMT, CTO Norfolk County Council and Chair Socitm (East)

Common risks that public bodies find when they examine their cloud usage include:

- More cloud apps in use than known about previously, often in 'shadow IT'.
- An increased dependency on internet connectivity and capacity.
- Many apps with no clear data ownership.
- Data use is not understood or tracked, with potential GDPR implications.
- Data is not guaranteed to be deleted when a service ends.

The CIO should concentrate on security of data and control of technical environments, but also consider wider risks, such as the huge growth in home working, and their mitigation in selecting a cloud supplier.

Cloud services – **managing** the risks

Business

- Interface and access, ease of use
- Continuity and resilience, as part of infrastructure
- Governance and reporting integrated
- Reference sites and case studies proven
- Exit clauses and other 'small print'

Technology

- Support e.g. transition capacity and skills transfer
- Standards, compliance and wider IT 'know-how'
- Innovation and ideas to ensure sustainability
- Integration, implementation and problem solving

Finance

- Hidden costs and future cost protection
- Value for money: current and future benchmarks
- ROI targets – evidence of realism and practicality
- Cost of change, backed up by client references
- Ongoing revenue and capital costs defined

Data

- Security, data protection and GDPR compliance
- Data recovery planning and data independence
- Access management design and federated identity
- Data policies and advocacy

At the same time, it is easy to overstate the security risks.

For example, findings from research by Calligo and Intel[5] indicate that:

> *"44% of CIOs... admitted that they had made compromises in the commercials in order to accommodate their security preferences."*

The public sector is, by its nature, risk averse. It has to be – the public scrutiny, political oversight and press appetite for failure in the public sector all require a cautious approach. The public sector also holds a great deal of sensitive and valuable data. It is there to support vulnerable people and to look after their needs, as well as those of local businesses and the wider community, and must protect digital services and the data they use about these groups.

A failure in security or the technical environment of a cloud project could have more serious human consequences than in many private sector scenarios.

This is not a reason for avoiding cloud, but a reason for ensuring that risks are understood and mitigated.

Cloud services – **mitigating the risks**

Business

A clear cloud adoption policy, IT architecture and redefined IT strategy will help to ensure that the business costs and risks can be more readily quantified. But CIOs will also need to establish how a cloud provider will deliver a service – governance, reporting, data tracking and recovery.

Finance

Mitigation of financial risks comes from a rigorous and agreed approach to business case construction for cloud services across the organisation. The CIO will need to work with service departments on specific cases and with the CFO on a general format for benefits quantification and realisation of cloud benefit.

Technology

The best approach to technology risk mitigation is to redefine the corporate IT strategy. It is not enough to bolt a cloud vision into an existing IT strategy and hope that technical risks and complexities can be identified and managed when needed. An integrated IT strategy will focus on IT capacity and capability risks.

Data

There are two aspects to this, the first being a corporate approach to information and data management, against which a cloud solution can be validated, and the second lies in having a technical architecture of how cloud services will connect to corporate infrastructure and comply with standards.

6. Some technical considerations for CIOs

There is nothing complex about cloud in terms of technology use or impact. Many of the design aspects of traditional IT delivery apply equally to cloud provision. But a move to a predominantly cloud model of IT delivery does require careful consideration by the CIO.

Some of the areas to consider, include:

IT resources
IT costs of change, training, efficiency and productivity gains, infrastructure capacity pressure

Security
Data protection, access design, federated identity, IT risk monitoring, testing, resilience

Avoiding 'lock-in'
Open APIs, common standards, open data and non-proprietry platforms

Technical support
Escalation and IT problem management, helpdesk, migration, testing

Integration
Identify common technology dependencies, linked data and integration

Data
Compliance, GDPR sharing, location, processing methods, data sensitivity classification

Consideration needs to be given to how IT operations are carried out as much as reconfiguring the IT strategy. Common terms such as 'Platform as a Service' (PaaS) and 'Government as a Platform' (GaaP) should also be defined. Many cloud terms originated in the USA and were adopted by HMG's Government Digital Service (GDS) as strategic ambitions for Whitehall a decade ago. Whilst helpful, these terms also typically need explaining in the context of, say, a diverse local authority.

CIOs need to be confident in defining their approach, not simply copying a popular idea. For example, the organisation may be better off adopting 'Software as a Service (SaaS) for key line of business applications but on-premise for some smaller or more sensitive systems.

If 'cloud' is simply added into an IT strategy, perhaps as a stated ambition of a 'cloud first' approach, it is likely that cloud benefits will fall short of expectations or could lead to poor performance, technology or data risks, hidden costs and the rise of shadow IT, as users seek a workaround method resulting in a 'free for all'.

Instead, the IT Strategy will need to be rewritten and repurposed for cloud, especially if cloud is to become the dominant delivery vehicle for IT services. In particular, the strategy must have a heavier focus on data, exit and change planning, supplier management and security architectures that protect systems, services, and information.

Within this revised approach there is an implied adjustment to the role of IT to become a provider of connectivity and a channel to access data, with particular emphasis on service management and data controls rather than provision of processing capacity and capability.

Areas such as perimeter security design, micro segmentation and zero trust networks, in particular, will need to be reviewed, along with configuration, capacity planning and resilience. Ensuring cloud services conform to these relevant standards will help to simplify migration considerably.

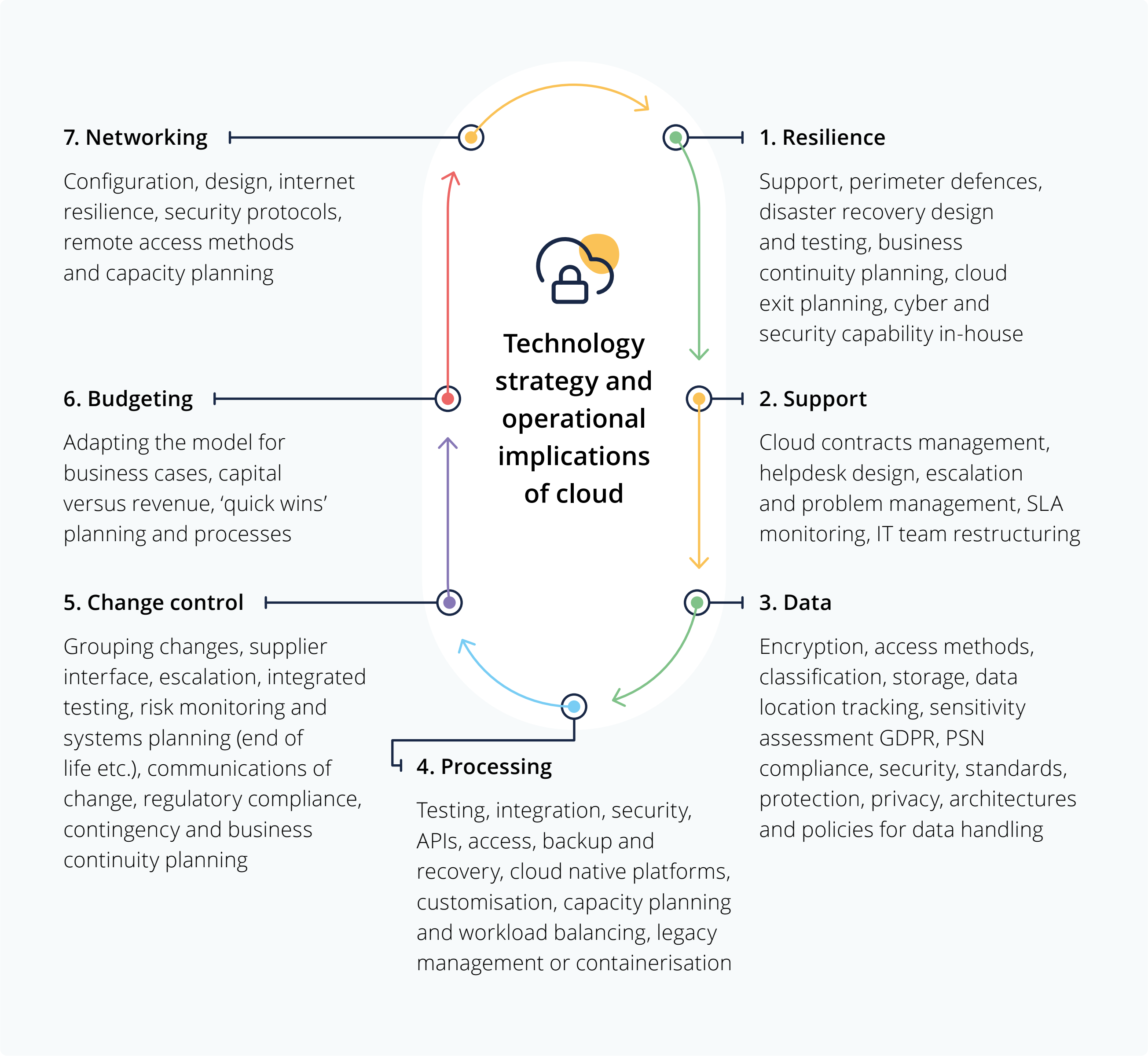
Cloud industry-recognised standards

There are just too many to list, but some of the key examples include:

- ISO27001 information security management
- ISO27017 security controls for cloud services
- IOS27018 personal data in cloud environments
- Cloud security alliance (CSA) STAR
- Cyber Essentials and Cyber Essentials Plus

There is also a technical challenge for IT in deciding how to deal with legacy applications and whether to re-architect these for the cloud, starting with consideration of how cloud services are to be accessed by the user and connected, particularly in a hybrid model. This could be done using 'container architectures', for example, but is also likely to require stronger security and workload rebalancing.

For many organisations however, the preferred route (and maybe the only option) is to retain legacy applications and gradually retire these when a cloud alternative becomes available and dealing with legacy becomes viable (risk, cost and complexity permitting).



Technology strategy and operational implications of cloud

1. Resilience

Support, perimeter defences, disaster recovery design and testing, business continuity planning, cloud exit planning, cyber and security capability in-house

2. Support

Cloud contracts management, helpdesk design, escalation and problem management, SLA monitoring, IT team restructuring

3. Data

Encryption, access methods, classification, storage, data location tracking, sensitivity assessment GDPR, PSN compliance, security, standards, protection, privacy, architectures and policies for data handling

4. Processing

Testing, integration, security, APIs, access, backup and recovery, cloud native platforms, customisation, capacity planning and workload balancing, legacy management or containerisation

5. Change control

Grouping changes, supplier interface, escalation, integrated testing, risk monitoring and systems planning (end of life etc.), communications of change, regulatory compliance, contingency and business continuity planning

6. Budgeting

Adapting the model for business cases, capital versus revenue, 'quick wins' planning and processes

7. Networking

Configuration, design, internet resilience, security protocols, remote access methods and capacity planning

As services gradually migrate to externally hosted public cloud provision, the role of IT will shift to 'cloud application service broker' tasked with balancing risks of data compliance and functionality with the benefits. In summary, it is a shift for the CIO from being a custodian of data processing to a custodian of data.

There is likely also to be pressure to adopt supplier SLAs for support and change control, resulting in loss of control by client services, a move away from immediacy of response from an in-house team, etc. This will need particularly careful planning to ensure that the management of change considers the wider impact on other systems and service provision.

Initially, many organisations may start with a blend of 'hybrid' and 'private' cloud and gradually migrate to 'public' cloud models, with a redefined 'front door of access', underpinned by clearly defined principles, architectures and policies to preserve access control.

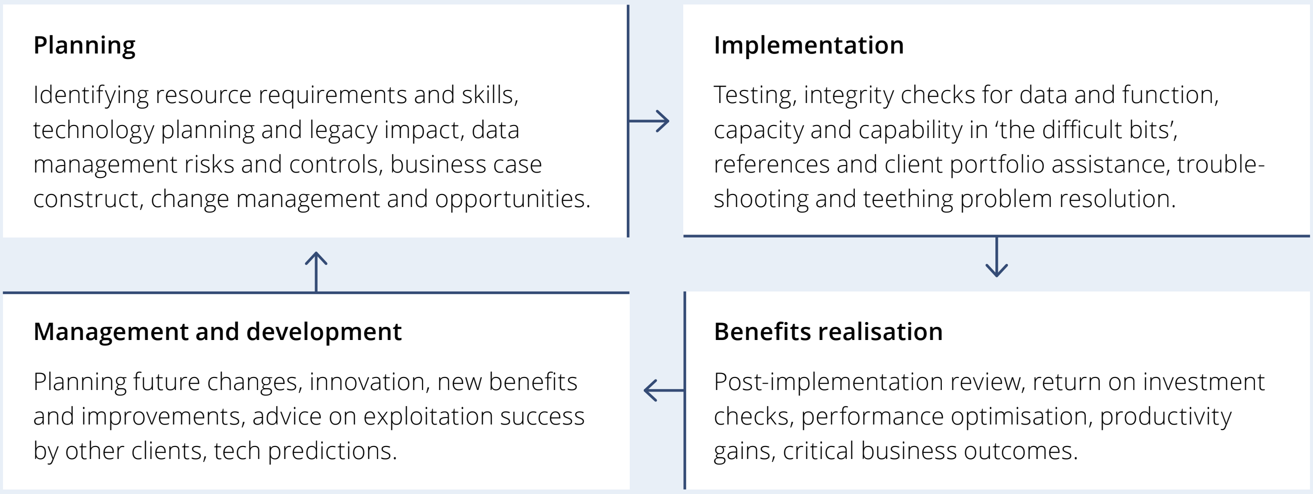
Ideally CIOs should be looking for cloud service providers for complex, strategic areas of service delivery, to assist in the whole lifecycle of a solution, not just its implementation. Providers will often have a relevant insight into technology futures, risks and opportunities, as well as knowing the best way to deploy and exploit their product, and this should be harnessed.

Some recent cloud adoption statistics:

- 90% of companies are on the cloud
- 60% of workloads were running on a hosted cloud service in 2019 (45% in 2018)
- Amazon Web Services is the leading cloud supplier with a 32% share.
- Cloud data centres will process 94% of workloads in 2021
- The average business runs 38% of workloads in public and 41% in private cloud.
- Hybrid cloud adoption is 58%.
- About a third of companies' IT budget goes for cloud services.
- AWS and Azure are the vendors of choice for 93% of cloud beginners.

Ref: hostingtribunal.com (compiled from various sources[6])

How can a Cloud Service Provider assist the public sector?



Planning

Identifying resource requirements and skills, technology planning and legacy impact, data management risks and controls, business case construct, change management and opportunities.

Implementation

Testing, integrity checks for data and function, capacity and capability in 'the difficult bits', references and client portfolio assistance, trouble-shooting and teething problem resolution.

Benefits realisation

Post-implementation review, return on investment checks, performance optimisation, productivity gains, critical business outcomes.

Management and development

Planning future changes, innovation, new benefits and improvements, advice on exploitation success by other clients, tech predictions.

7. Choosing a cloud service partner

In choosing a cloud service partner (CSP), the first step is to ensure that you have a set of clear business and technical requirements for the cloud service.

A number of councils we spoke to for this research maintain a clear set of cloud principles that support the IT strategy and digital plans of the organisation. These then form the basis of supplier requirements above and beyond functionality. They fall into two groups:

- Expectations for the specific cloud service being acquired
- General expectations of cloud suppliers to the organisation.

There is often a focus on defining specific supplier requirements, but it is important for the CIO to ensure that these are set within the context of an overarching IT strategy and architecture.

> *"Cloud is often sold as a 'product' rather than a 'service', masking the true costs over time – especially if promoted as an easily administered solution. Many local authorities are being caught out through lack of knowledge on initial provisioning of services and poor oversight on costs of usage. This is often caused by the over-promotion of value and a lack of investment in skills to monitor, manage and administer the service."*
>
> Kevin Taylor, Head of ICT, West Sussex Council

In addition, the organisation should be looking for a cloud service provider able to deliver more than a basic cloud service (whilst recognising that there are different types of providers as well as solutions offered).

Cloud service providers

- **Systems integrators,** helping you to navigate a multi-cloud environment, designing cloud application platforms and managing the relationships with cloud platform providers.
- **Tool providers,** who deliver a range of functionality, from cloud optimisation and load balancing, to specific cloud-based applications.
- **Partners to manage cloud programmes,** who typically provide cloud expertise and resources, including set-up and governance.

Client expectations

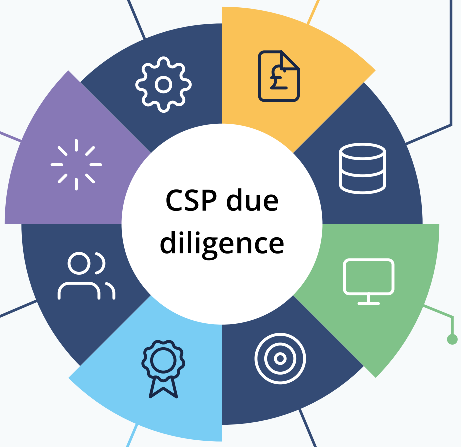
- CSPs can have a key role in supporting migration and helping to accelerate the cloud journey, including business case development and benefits realisation.
- CSPs should bring experience from multiple clients of the risks and pitfalls, and how to spot them, mitigate and overcome them.
- CSPs should also offer high levels of data management and security alongside a highly resilient and flexible service.

In tendering and selecting a cloud service, even for a simple and specific need, due diligence checks are essential and go beyond functional adequacy. Several CIOs interviewed for this research suggested that greater consideration of the supply of data on carbon footprint and standards for data ethics were going to become key criteria in selection processes in future.

Procurement routes for cloud services also vary. Some cloud apps are effectively free to use or very low cost and require limited tendering. Others require more formal acquisition. The G-Cloud framework on the GOV.UK Digital Marketplace is a useful procurement mechanism for all public service organisations, especially central and local government.[7]

Even for small scale cloud acquisition, where services may only be seen as temporary or non-strategic, CIOs need to be sure that the risks and benefits are understood, since these systems will still have network connections and hold valuable data.

Checks should include a range of factors in a due diligence CSP assessment.



Migration support & exit

This includes support for transition and migration – capacity, capability to complement internal skills gaps and risk mitigation and avoiding being locked into proprietary technologies.

Commercials & contract

VFM tests should be covered in the specification, but there will be the need to check the CSP's business and financial health, T&Cs for contract renewal or exit, as well as dependencies on other third party suppliers. Check pricing models with care.

Innovation & value add

Many CSPs will offer more than the basic tendered requirements – find a way to put a value on intangibles such as innovation and enhanced ongoing technical or business support offered.

Data policies

Arguably, the most important factor, this includes the CSP's approach to data processing, data location, GDPR compliance, backups, patching policies, DR and security provisions. Make sure that your data architecture and classification schemes are not compromised by the CSP's methods.

Credentials

Beyond the commercial checks and standards, consider factors such as corporate social responsibility, code of practice, ethos and public service alignment in your chosen CSP.

Reliability & performance

Check if SLA performance claims can be proven and how issues are managed and escalated. Avoid suppliers with long chains of invisible dependencies on other providers.

Standards & accreditations

There are many standards for cloud services, but start with ISO27001 and Cyber Essentials Plus for security compliance. Look for recognised cloud service standards, such as those recommended by the NCSC and PSN compliance.

Technology roadmap

This about aligning with your internal IT strategy, current environment and digital priorities, as well as the supplier having a credible roadmap of developments. Consider configurations, recoding and testing required to migrate workloads to the cloud.

G-Cloud framework

There are around 31,000 cloud services on the G-Cloud framework, hosted in the Digital Marketplace (an 'online store', previously called 'CloudStore').

Despite its original design for Whitehall use, the G-Cloud framework is increasingly used by local government in particular to reduce time and cost overheads of IT procurement.

Councils should ensure that the G-Cloud framework, now in its 12th iteration, is an accepted and preferred procurement route for technology acquisition in their own organisations.

It is a mistake to start looking at suppliers and systems before understanding either the business problem that is being addressed, or the wider context for a multi-cloud environment that depends on standards and compliance. This includes being clear on your current IT and business cost profile and being clear on client-supplier contractual arrangements and support.

By having a coherent approach to cloud sourcing assessments, it is easier to establish the maturity of approach, skills, methods and architectures employed by a proposed cloud supplier. Ideally, a cloud partner will help to manage complex integration issues and to source solutions for problems that arise when you have a multi-cloud environment, whilst recognising that you cannot 'outsource' problems without a clear and mutually agreed plan to address them.

8. Service integration and management (SIAM), and cloud

Historically, an IT department would run a data centre, develop programs and oversee networks. This role progressively reduced, as packages of software became available, hardware maintenance became more sophisticated and IT outsourcing became popular.

With the IT department becoming more dependent on external expertise and support, it has had to become more skilled at selecting and managing IT suppliers. With a growing multiverse of cloud services, this has become even more challenging.

The IT team may also be responsible for legacy on-premise systems, outsourced contracts, and a range of new IaaS cloud services. This environment requires a structured method to manage the supply chain process in a growing tangle of multi-sourced services.

'Service Integration and Management' (SIAM) addresses the problem of the growing cloud multiverse. Whilst there are suppliers who offer SIAM as a service, it can (and is often) undertaken in-house by the IT team. SIAM methods will ensure that:

1. **There is a structured approach to identifying IT suppliers:**

   - Data held and business purpose
   - Contractual details and renewal points
   - Dependencies on other resources
   - Escalation routes and problem management

2. **Coordination of change control and upgrades takes place:**

   - Communications
   - Risk management and identification
   - Data and test planning

3. **Service management and performance are integrated and consistent:**

- Benchmarking
- Assessment of benefits realisation

4. **Higher levels of compliance with ITIL and other standards:**

- Data breaches, risks or issues
- Future planning

These are all standard IT team management practices, but they become more challenging in a highly externalised cloud environment, where traditional IT supply management techniques are potentially too difficult and cumbersome.

For example, it is unlikely to prove possible to get all suppliers to follow the same processes and practices. Also, the IT team may have to deal with different parts of their organisation that have set up their own working relationships with different cloud suppliers, so that coordination will be harder and reporting on performance and monitoring risks can be time intensive.

CIOs should start with the most strategic cloud services based on business priority, the data being processed and level of risk. There are methods to assist with this, such as the Kraljic Matrix.[8]

9. Defining data requirements

Assuming the organisation already has a comprehensive data classification scheme in place that defines policies on data use and sharing, alongside classification and allocation of data sensitivity, then it is not too difficult to apply this to a CSP offering.

It is also important to check rather than assume that the CSP's policies comply with GDPR, specifically in areas such as breach notification, data encryption and security practices. Checking out the escalation process and staff training can be helpful. Areas such as data ethics, the CSP's use of third parties, staff training, and track record are also important to consider.

Security remains the main worry for most organisations in any sector in considering a migration to cloud solutions. Having a set of pre-defined data security and data handling principles can act as a checklist for assessing a proposed cloud service offering, including knowing where data is being held at all times.

Checking a cloud supplier's data practices

- Able to verify data deletion is completed
- Encryption of data in transit
- GDPR compliance demonstrated in full
- Data sharing and third party involvements
- Data processing locations
- No risk of 'hopping' between different client areas
- IT security arrangements in general documented
- Validated security and data standards and compliance
- Infrastructure resilience being independently tested
- Processes if a data breach occurs
- Business continuity and disaster recovery procedures
- Access management processes
- What are the policies for service staff including vetting and training?
- ISO27001 and Cyber Essentials accreditation

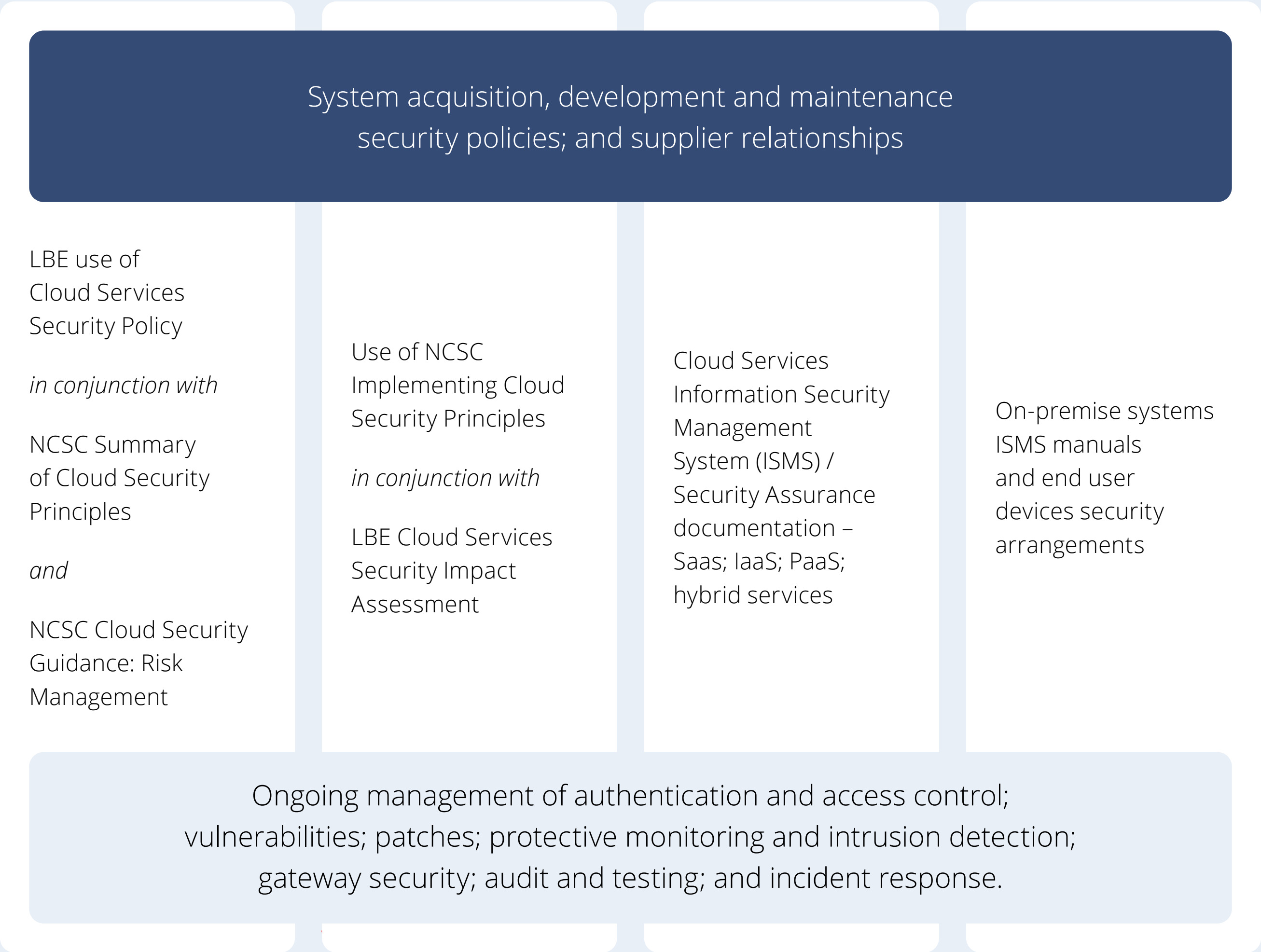
Source: Government cloud security principles (bit.ly/2N2M6zW)

CIOs need to look no further than the National Cyber Security Centre's '14 principles' guidance,[9] even if these are adjusted, based on the local context. Appendix B summarises the main guidance from the NCSC on how to deploy cloud services securely. There are also some good sources of cloud security policies from local councils, such as this example from the London Borough of Enfield:

Use of cloud services security policy

ENFIELD Council

No cloud service should be consumed as a live service until the applicable security requirements in each pillar described below have been considered.



System acquisition, development and maintenance security policies; and supplier relationships

LBE use of Cloud Services Security Policy

in conjunction with

NCSC Summary of Cloud Security Principles

and

NCSC Cloud Security Guidance: Risk Management

Use of NCSC Implementing Cloud Security Principles

in conjunction with

LBE Cloud Services Security Impact Assessment

Cloud Services Information Security Management System (ISMS) / Security Assurance documentation – Saas; IaaS; PaaS; hybrid services

On-premise systems ISMS manuals and end user devices security arrangements

Ongoing management of authentication and access control; vulnerabilities; patches; protective monitoring and intrusion detection; gateway security; audit and testing; and incident response.

10. Where to start a cloud journey

It is tempting to adopt new cloud services as business leaders request or as suppliers dictate, or simply because the IT strategy says: 'cloud first'.

In practice, many public service organisations will already be deploying some cloud services and may already be struggling to make sense of an incoherent cloud collection that has grown unchecked. Ideally, the CIO needs to be prepared by building an agreed architecture for cloud adoption and a checklist of risks and pre-adoption checks, as already described. Typically, this falls into three broad activities.

Planning a move to cloud services

1. Develop a hybrid cloud strategy
   - Review the current application portfolio to identify issues in value, flexibility, data quality, integration, usability etc. This will help with cloud migration prioritisation.
   - Define a security and network architecture and context for cloud adoption, including standards, connectivity, integration needs, resilience and support.
   - Consider existing datacentre arrangements – skills, partners, core technology, capacity. This will help to define the balance between public, private and hybrid cloud models.
   - Review disaster recovery and business continuity planning in the context of cloud delivery. This will help to plan cloud testing, resilience planning, emergency recovery.

2. Address legacy infrastructure
   - Redefine legacy infrastructure to be built around a private cloud model (IaaS). This will create a number of changes in methods, processes, risk management and skills in IT.
   - Identify the full 'Total Cost of Ownership' (TCO) of the legacy estate to support the business case for cloud migration where possible.
   - Move core systems (Office, ERP, CRM etc.) to cloud provision – public cloud where possible. These applications are better provisioned in the cloud.
   - Establish a plan for legacy applications that cannot migrate to cloud – retire, replace, or use a cloud 'wrap' to retain if unavoidable, but within a modern architecture.

3. Define, share and agree benefits and inhibitors
   - Define the basis on which cloud benefits will be measured above and beyond the IT department and costs.
   - Involve finance and other business colleagues in determining how cloud benefits can be realised by linking to business performance outputs.
   - Establish a firm basis for cloud business case development, including addressing the change from Capex to revenue-based IT spend.
   - Identify IT and digital innovation benefits of cloud specifically (access to new, modern tools at lower cost) and how these can help to transform or improve business activity.

This assumes good existing control of the organisation's overall software portfolio.

In migrating to a public cloud, there are eight key considerations for the CIO:

1. Determining which workloads to move to the public cloud, based on complexity, risk, and security requirements.
2. Checking the marketplace – are there cloud service providers out there able to meet the requirements?
3. Prioritise based on risk cost and benefit. Don't start with the most difficult.
4. For each data set, system and workload, determine the appropriate level of security required.
5. Determine the level of controls and integration required for the individual cloud application.
6. Assess against your existing architectural standards the level of compliance achieved by the proposals available.
7. Determine the controls and governance models required and their deliverability.
8. Select a cloud service provider that meets the wider requirements of the organisation where possible.

At a more detailed level, CIOs are recommended to document as simply as possible the areas that can help to identify the priorities and the risks for cloud migration:

Define the basic architecture and principles of cloud adoption, including the vision for cloud (e.g. establishing priority areas for adoption and a 'cloud first'/'public cloud first' policy). Also, how the architecture will be amended and developed as requirements require.

Define the standards to which cloud solutions must conform, whether private, public or hybrid cloud – both basic cloud standards and the standards that will ensure the integrity of the wider IT architecture. This includes scalability as well as cyber security and authentication.

Define the expectations of cloud suppliers – ethos, data practices, support, resilience, etc. It is important to choose the right partners. This includes the stewardship of public data and GDPR compliance.

Define the organisation's road map for cloud adoption – dependencies, priorities, funding, time line, contribution to digital transformation aims etc. This includes operating model impact.

Define the basis for cloud business case modelling, noting the need to offset increased revenue overheads against capital savings and revenue savings in business areas, not just IT.

> *"I think there is a certain inevitability to cloud adoption once one appreciates that cloud native tools, combined with the right culture, will always deliver a better service to the customer than traditional IT methods.*
>
> *To make an informed decision about cloud adoption, it is useful to gain an understanding of DevOps. In many ways cloud computing and DevOps are inextricably linked.*
>
> *Whether you are thinking about cloud adoption for the IT Service within a local authority or the software development processes of one of your key software suppliers, the culture will be a vital aspect of successful adoption."*
>
> **Tony Doyle**
> Head of ICT Blackpool Council

Define the nature of business change expected to exploit the benefits of cloud (and, where necessary, to mitigate risks).

Define the security and resilience requirements of cloud solution. This is not the same as basic standards, and is about the appropriateness of the specific solution for the nature of the data and systems functions in the context of public service delivery.

Where possible, in a major cloud development project, start small and undertake a proof of concept to demonstrate the functionality and iron out 'wrinkles' before scaling up to the full implementation. Your CSP should assist with this.

In-house IT skills will also need early consideration, since cloud demands a range of new challenges, such as deploying 'containers' or 'Kubernetes'[10] to migrate workloads across clouds.

> *"I think all of us in the public sector are quite a way along our journey towards the cloud. At this point in time, we have already taken a view on the benefits of cloud and its place in our infrastructure, and this is iteratively reviewed.*
>
> *For me, cloud is not an end in itself, it is just one of the many technologies that we use to deliver value to our customers."*
>
> **Sandra Taylor**
> Assistant Director of IT & Digital,
> Worcestershire County Council

Conclusion

Cloud offers significant benefits for all organisations, and particularly smaller organisations that can access innovative and flexible technology at much lower cost than would otherwise be possible.

The benefits of cloud are widely understood, both in terms of potential cashable savings and business value. However, the evidence suggests that to realise these benefits, organisations need a clear plan for their cloud journey, whilst accepting the need to adapt and change along the way.

This plan is not just for IT and requires public services to resist buying individual cloud services as point solutions, without having a policy and strategy for cloud. This should replace a traditional IT strategy and embrace an outcome of wider business changes in order to realise value and to manage cloud risks.

Cloud supply due diligence is also critical , ensuring that selection criteria go beyond functional requirements and include the supplier's approach to data management, data exit strategies, compliance and standards. Organisations with weak governance are likely to end up with a patchwork of cloud solutions or pressure for unnecessary customisation and tailoring that will become a legacy headache in the longer term.

The CIO can help with the wider organisational understanding by turning the jargon into practical and relevant interpretations. Terms such as Government as a Platform (GaaP), Platform as a Service (PaaS), 'Cloud First', 'hybrid/public/private cloud', and so forth, need to be explained in a simple cloud policy.

With the right foundations, cloud in the public sector can be truly transformative, supporting shared service, flexible working and a move away from constrictive and expensive legacy IT. By operating on common, standardised microservices, public services can construct automated customer-focused, end-to-end processes, which are secure, resilient and adaptable.

The public sector CIO should treat cloud as an enabler, not as an ambition in its own right. Cloud is turning much of data-processing into a utility, and the emphasis moves to identifying the best way to transport and harness information securely, efficiently and effectively. We anticipate that most future systems functions will be public cloud based. The IT department will need to reinvent itself and the IT strategy in readiness for this.

As a cloud service broker, the public sector CIO can ensure not just that the right mix of cloud solutions are acquired to maximise the benefits, but also that the associated business risks are understood and well-managed throughout the wider organisation.

> *"Cloud is a key component of our technology architecture, enabling us to support our workforce to work remotely as well as underpinning next-generation technologies such as AI.*
>
> *Many public sector organisations will continue to have a hybrid environment for some time to come, given the scale of their operation, diversity of services provided and existing infrastructure investments. Our cloud strategies need to align with our council priorities, optimising the balance between on-premise, edge-based, public cloud and hybrid-based services, whilst at the same time ensuring agility and security in our enterprise."*
>
> **Sandra Taylor**
> Assistant Director of IT & Digital,
> Worcestershire County Council

References

[1] Edge computing – Wikipedia: bit.ly/37hSCcX

[2] Cloud outcomes survey: Expectation vs. reality – Accenture: accntu.re/3qoThAO

[3] Government adopts 'Cloud First' policy for public sector IT – GOV.UK: bit.ly/2ZgcGYN

[4] UK councils opt for hybrid cloud, report finds – GovTech Leaders: bit.ly/3ddu4Fx

[5] Security, compliance and cloud strategy at the IT Leaders' Summit – Calligo: bit.ly/3pmV5ZK

[6] 25 must-know cloud computing statistics in 2020 – Hosting Tribunal: bit.ly/2OJa0AT

[7] G-Cloud buyers' guide – GOV.UK: bit.ly/3u3n4Bm

[8] What is the Kraljic Matrix? – Forbes: bit.ly/3b9s6Ua

[9] NCSC Guidance on how to configure, deploy and use cloud services securely – NCSC: bit.ly/2ZfLbhQ

[10] Kubernetes – Wikipedia: bit.ly/3pplYft

Appendix A

Common cloud myths

On-premise is always cheaper

Analysis of 'total cost of ownership' will typically show that there are significant cost advantages in public cloud solutions over privately owned equipment 'on-premise'. But the trade-off is not that simple, and there are fewer tangible factors, such as technology control or digital maturity that might make an on-premise solution lower cost overall at a point in time.

Public cloud is always cheaper

There are many cost advantages of public cloud, but typically these diminish if the cloud solution required is complex, or where a significant degree of customisation is expected. There are also potentially additional costs, at least initially, in moving significant business-critical workloads to a public cloud model.

Cloud is always cheaper:

Cloud offers potential savings, but this is not always the case, and a simplistic 'cloud first policy' is often risky. Cloud is most efficient when consumed as an 'off the shelf' public cloud service, where business activity is configured to optimise functional value of a cloud model. If this is not feasible (and there are many reasons why this may be the case) then cloud may not be the cheapest option.

Cloud is more expensive

Some CIOs can prove the efficiency of their in-house data centre or current outsourcing arrangements over cloud, especially where there are specialist or data-sensitive applications that have been optimised for the business. At the same time the on-going legacy costs of such designs needs to be carefully monitored as cloud services mature and legacy IT costs increase.

There is only one cloud

As this report describes, there are many types of cloud models, from recognised and less well-known suppliers, each with their own infrastructure. CIOs need to ensure they understand the technical and business model of the cloud multiverse they are building (or acquiring), wherever its source.

Every cloud service is different

There is consolidation happening in the cloud marketplace. A number of key suppliers are dominating, and many of the recognised cloud services are run on the same foundations (such as AWS or Azure). For the CIO the importance of this is not only in ensuring that they know where data processing is taking place and by whom, but also that they can watch the small print in terms of changing cost profiles of a cloud service .

Appendix A (continued)

Common cloud myths

Cloud is digitally transformative

It is true that a cloud model for delivery can help to transform and deliver true digital working, but too often a cloud solution is acquired as an incremental improvement in IT delivery rather than a fundamental shift in how the organisation functions. In other words, cloud is only transformative if the organisation chooses it to be so.

Cloud is just an extension of traditional IT

When a cloud service is acquired as a new system, it may require little or no change in IT delivery beyond new skills involved in the implementation and testing. But over time as a cloud multiverse consumes traditional IT practice it is likely to force a rethink in how IT functions. Better is to redesign IT before cloud adoption reaches this state.

Cloud is less secure than on-premise

Cloud security remains the main reason why some CIOs are apprehensive about cloud adoption. Concerns include: fragmentation of the IT architecture, data protection and systems access being compromised or at risk. Whilst the worries are real, it is also true that the main IT suppliers operate at such scale and investment, with so much at stake in their reputation for security and resilience, that they offer more secure services than any on-premise solution could afford to be.

Cloud is more secure than on-premise

Whilst the basic cloud security and resilience of the big cloud suppliers outstrips a typical in-house solution, there is more to security than the resilience of the platform. CIOs need to check out a range of criteria to be reassured that a cloud service is as secure as they need, especially as most security breaches are from human error, not machine failings. Suppli-ers interdependencies may need to be assessed as well in the delivery model. It is also true that a proliferation of security tools needed to manage many cloud suppliers can increase risk.

Multi-cloud reduces vendor lock-in

Some CIOs are concerned that if they depend on one of the major cloud suppliers, such as Google, Microsoft or Amazon, they are more vulnerable to 'lock-in'. There is a risk, and not just for the main platforms but for many of suppliers selling a suite of solutions. However, lock-in comes from things such as proprietary standards and weak contracts, and that applies in a multi-cloud scenario as much as a single vendor platform.

Multi-cloud increases vendor lock-in

An organisation can inadvertently create their own 'lock-in' by acquiring many different cloud solutions that inter-depend, so that replacing any one of them can create real difficulties. This can be compounded if there is no strong standardisation of approach in cloud adoption, or enforcement of technical standards and architectures from which to ensure strong corporate compliance.

Appendix B

Guidance on how to configure, deploy and use cloud services securely – NCSC (bit.ly/2ZfLbhQ)

9. **Data in transit protection**
   User data transiting networks should be adequately protected against tampering and eavesdropping.

10. **Asset protection and resilience**
    User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.

11. **Separation between users**
    A malicious or compromised user of the service should not be able to affect the service or data of another.

12. **Governance framework**
    The service provider should have a security governance framework which coordinates and directs its management of the service and information within it. Any technical controls deployed outside of this framework will be fundamentally undermined.

13. **Operational security**
    The service needs to be operated and managed securely in order to impede, detect or prevent attacks. Good operational security should not require complex, bureaucratic, time consuming or expensive processes.

14. **Personnel security**
    Where service provider personnel have access to your data and systems you need a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service provider personnel.

15. **Secure development**
    Services should be designed and developed to identify and mitigate threats to their security. Those which aren't may be vulnerable to security issues which could compromise your data, cause loss of service or enable other malicious activity.

16. **Supply chain security**
    The service provider should ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement.

17. **Secure user management**
    Your provider should make the tools available for you to securely manage your use of their service. Management interfaces and procedures are a vital part of the security barrier, preventing unauthorised access and alteration of your resources, applications and data.

18. **Identity and authentication**
    All access to service interfaces should be constrained to authenticated and authorised individuals.

19. **External interface protection**
    All external or less trusted interfaces of the service should be identified and appropriately defended.

20. **Secure service administration**
    Systems used for administration of a cloud service will have highly privileged access to that service. Their compromise would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data.

21. **Audit information for users**
    You should be provided with the audit records needed to monitor access to your service and the data held within it. The type of audit information available to you will have a direct impact on your ability to detect and respond to inappropriate or malicious activity within reasonable timescales.

22. **Secure use of the service**
    The security of cloud services and the data held within them can be undermined if you use the service poorly. Consequently, you will have certain responsibilities when using the service in order for your data to be adequately protected.

About this report

Author
Jos Creese - Independent, digital consultant, researcher and analyst

Editor
Martin Ferguson - Director of policy and research

Designers
Magdalena Werner - Senior creative designer
Benjamin Hughes - Graphic designer

Have your say

We always welcome feedback and discussion on the contents of our publications.

Martin Ferguson
Director of policy and research
martin.ferguson@socitm.net

Nadira Hussain
Director of leadership development and research
nadira.hussain@socitm.net

Get in touch

Website: www.socitm.net
Email: inform@socitm.net
Tel: 01604 709456

Join the conversation... @Socitm | Socitm