How to adopt cloud for digital government success

How to adopt cloud for digital government success

The UK Government has provided clear direction on increasing the adoption of cloud in the public sector as part of its digital strategy. This guide examines the progress made, gives practical advice to those tasked with delivering cloud solutions, and highlights key considerations based on Cisco's work with the public sector and our cloud vision.

The 2012 launch of the Government Digital Strategy set out to redesign transactional services to meet a new digital by default standard.

The standard sets out to deliver simpler, clearer and faster services online that are designed around the needs of the citizens and businesses that use them.

The Digital Strategy includes several key action points for central government and the broader ecosystem of public sector entities to promote agility, openness and innovation.

Ultimately, moving public services to digital is expected to save the Government £1.7 – £1.8 billion each year.

More recently, the Cabinet Office launched the Government Transformation Strategy 2017–2020. This extends the previous commitment and places the UK Government as a world leader, currently first in the 2016 United Nations E-Government and E-Participation survey.

> ***"We will transform the relationship between citizens and the state – putting more power in the hands of citizens and being more responsive to their needs."***
>
> **Ben Gummer**
> *Minister for the Cabinet Office and Paymaster General, July 2016-June 2017*

Embracing cloud

The adoption of cloud is identified as the most significant investment pillar within digital transformation initiatives[1].

In the UK, a study by IDC found that 63% of organisations are already using some form of cloud (private or public). The study revealed that cloud adoption is enabling the digital transformation of public sector services to deliver economies of scale, faster time-to-market and increased flexibility.

Since 2012, the UK Government has embraced and promoted the adoption of cloud by public sector entities. For example:

- **The G-Cloud framework** has created a Digital Marketplace of vetted suppliers that has significantly reduced the complexity and duration of the procurement process for cloud solutions. It also provides small and medium-sized enterprises (SMEs) with the opportunity to serve public sector organisations.
- **The Cloud First policy** – a directive stating that purchases through the cloud should be the first option considered by public sector buyers of IT products and services, published under the 2010 to 2015 Conservative and Liberal Democrat coalition government.
- **Crown Hosting Data Centres** – facilities dedicated to the UK public sector for hosting applications and services (a common interpretation of cloud adoption and one of cloud's popular use cases is associated with outsourcing services mainly around application hosting). Central Government has been promoting such an approach with an asset-light strategy and is no longer building new private data centres.

These policies and initiatives have seen the UK public sector mature in its adoption of cloud services over the past four years, with a growing number of organisations embracing a cloud first strategy.

The Government now intends to accelerate the public sector's digital transformation journey by focusing on two pillars – cloud and networks.

> ***"Public sector organisations should consider and fully evaluate potential cloud solutions first – before they consider any other option."***
>
> **Cabinet Office,** *2013*

[1]IDC's Global IoT Decision Maker Survey,

From cloud first to cloud native

In early 2017, the Government Digital Service (GDS) announced its intention to encourage public sector entities to move from a cloud first to a cloud native model by replacing legacy applications with Software-as-a-Service (SaaS), or developing new ones using Platform-as-a-Service (PaaS) solutions. This strategic imperative aims to deliver a futureproof, Application Programming Interface-centric (API-centric) platform of reusable components.

Platform thinking has been at the centre of UK's Government since 2012 following the launch of the Gov.uk publishing platform. This has evolved into the notion of Government-as-a-Platform – an approach aiming to provide a suite of common tools and reusable application components such as Gov.uk Pay and Notify, to public sector digital teams, enabling them to build services for citizens and businesses faster and easier.

> ***"...We've begun to move away from the phrase 'Cloud First' and instead begin to think in terms of 'Cloud Native.' Cloud First is the policy we've agreed, but it's not our aspiration."***
>
> **Cabinet Office,** *2013*

Cloud myth-busting

'Cloud' is not a location. There is a common misconception that cloud is only about outsourcing or hosting applications (typically in the form of virtual machines) with a cloud hosting provider (IaaS). But that's just one cloud use case. Others include the use of cloud apps (SaaS) or developing apps in the cloud (PaaS).

There is no 'single cloud'. The modern business landscape is part of a multicloud world, where different apps, users and devices connect to different clouds. Similarly, 'moving to the cloud' means using cloud-based functionality to support business functions that can benefit from the transition.

In reality, adopting cloud is a digital transformation journey, unique to each organisation, relating to the modernisation of consumption and delivery of technology. In more mature adoption strategies, it is associated with changes in people and process, rather than just technology.

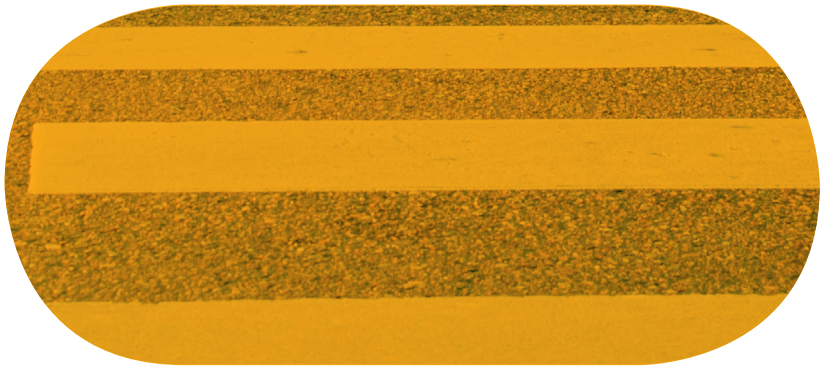
The end of the Public Services Nertwork (PSN)

The UK's PSN provided public sector entities with a single assured network for almost 10 years. Operated by multiple vendors, it gave access to services from accredited providers via a simplified procurement process.

Recently, the UK Government signalled its intent to move away from the PSN by stating that "The internet is OK" as the primary means of connectivity. Moving forward, new services and updated versions of older ones are to be published and accessed via the internet.

Moving away from the era of PSN is a necessary step towards accelerating cloud adoption. The PSN had come to be viewed as a layer of added complexity, unable to support a new generation of services consumed from multiple clouds. The GDS recognises there is now much work to do to develop the capability of the public sector to securely connect departments, users and devices and at the same time meet a set of basic standards.

Evolving the network layer is a necessary individual transition for every public sector department in order to accelerate cloud adoption in the post-PSN era.



UK public sector cloud maturity

The majority of public sector organisations remain in a transitional state in terms of moving away from the PSN and realising the GDS's cloud native vision.

However, for those looking to begin this journey, finding a set of solutions that can address a particular adoption phase means more than simply swiping a credit card. It calls for identifying a clear set of strategic goals and solid business case. It also requires an assessment of legacy technology and apps, culture, and skills etc. to understand current state.

Public sector organisations fall into one of three phases of adoption and exposure to cloud services (although larger organisations may have internal departments that span multiple adoption phases):

1: Little or no adoption of cloud

Organisations at this stage are employing private data centres and potentially using a small number of SaaS applications, with limited use of public cloud IaaS for application hosting and almost no use of PaaS. In this scenario, the networking infrastructure is 'private-centric': based on private managed Multiprotocol Label Switching/Wide Area Network (MPLS/WAN) services and Virtual Private Networks (VPNs) to access cloud services.

The user experience at these organisations can be impeded by infrastructure bottlenecks (mainly around networking) as cloud adoption increases. The lack of a consolidated security model for users and devices will increase risk, while the lack of visibility, automation and governance in terms of IT and line-of-business users may result in a rise in cloud service-related 'Shadow IT' incidents.

2: Increased IaaS adoption

More advanced organisations have established a preference for cloud services (consumed or hosted) for new applications. They actively avoid expanding their own data centre footprint. There may be some adoption of IaaS services for development, as well as for migrating applications (lift and shift), but it is not based on modern methodologies and PaaS offerings.

For organisations in this stage, access to cloud services could be enhanced via direct connections to specific clouds (such as AWS Direct Connect, Microsoft Azure ExpressRoute, and Google Platform Direct Interconnect), VPN services, or by using common edge solutions (e.g. Equinix Cloud Exchange). However, their network governance is more decentralised and 'off-premises' as a result. Potential risks include lack of control over the costs associated with access to different clouds, plus a lack of visibility and common centralised security policies across their networking infrastructure.

3: Aligned with cloud native

The most 'digitised' of public sector organisations are on their way to the UK Government's cloud native vision. These organisations embrace cloud services as their primary means for adding new applications. They also take a strategic view of migrating legacy applications to IaaS. A minority experiment with cloud native development using microservices-based application modelling and public cloud PaaS offerings.

The first prominent challenge for these organisations is the transition from the use of an MPLS network, which slowly becomes obsolete, to simply using the internet for access and general connectivity. As such, they need to find new ways of addressing security and governance mandates.

More importantly, those that embrace cloud platform tools completely must make changes in process and people. This can mean establishing DevOps operating models, shifting from Waterfall to Agile methodologies, and designing infrastructure and networking with self-service capabilities. Crucially, in all cases, it means acquiring new talent to support these models and capabilities.

A path to maximise the benefits of cloud adoption

Cloud promises many benefits. However, mapping tangible business outcomes to specific phases of cloud adoption calls for a universal methodology based on a large collection of data points.

A study conducted by IDC[2] found that the greater the level of cloud maturity, the better the business outcomes, including increased revenue and more strategic allocation of IT budget.

As shown in Figure 1, IDC identified five stages of cloud maturity. There are tangible and immediate benefits to be gained in terms of KPIs by progressing through these stages. For example, organisations with 'optimised' cloud strategies in the UK are realising on average £0.8 million in reduced costs per cloud application. Other benefits include faster provisioning of services and tighter alignment with internal service level agreements (SLAs).

For public sector organisations globally, the highest-ranking KPIs were:

- Reduction in IT operational overheads
- Enhanced customer experience
- Improved allocation of IT budget

The study also shows that more mature organisations have adopted cloud native methodologies such as DevOps, microservices-based development, containers and cloud-based IoT services. Using OpenStack was also found to drive expected business outcomes such as meeting SLAs and more strategic allocation of budget.

Although cloud adoption increased by 49% between 2015–2016 globally, with a majority pursuing a hybrid cloud strategy, only 3% of those surveyed had 'optimised' (more mature) cloud strategies in place. In the UK, this percentage was even lower (1%).

These findings underline the importance of being able to take a holistic approach to cloud adoption; understanding the starting point, destination and key strategic areas to address in each phase.

Figure 1: **5 STAGES OF CLOUD MATURITY**

[2]IDC White Paper, sponsored by Cisco, "Cloud Going Mainstream. All Are Trying, Some Are Benefiting; Few Are Maximizing Value". September

"It was clear that everyone agreed we could just use the internet... we're on a journey away from the PSN"

Government Digital Service,
2017

Four key considerations for your cloud strategy

Public sector organisations may see the advantages of going cloud native and moving away from the PSN, but they also recognise the risks and barriers they need to address before they can make the leap.

Some of the barriers are common to many areas of IT. For example, concerns around vendor lock-in and service performance issues.

Others are more often associated to cloud adoption. For example, concerns around data sovereignty, ensuring compliance with privacy directives and meeting service level agreements.

Although these concerns undoubtedly merit attention, they can also present opportunities as opposed to remaining barriers to cloud adoption.

1: The cloud security paradox

There is a common perception that the cloud is inherently less secure than traditional IT environments, especially if you add edge and IoT solutions into the equation. Yet cloud-delivered security offers great opportunities for better protection, ultimately showing how public sector organisations can use cloud services securely.

IDC highlights that those organisations with more mature cloud strategies are realising greater tangible benefits from cloud adoption and are more likely to consume cloud-delivered security services.

As depicted in Figure 2, those at the 'optimised' level of cloud maturity are twice as likely to use managed security services and consume cloud-delivered security for devices. But the real step change is that these organisations are much more likely to use cutting-edge cloud security technologies such as the mass-scale machine learning analytics services supporting rapid incident detection and remediation.

In a separate report[3], IDC asserts that modern public cloud architectures, built with Service Orientation in mind, offer natively more capabilities in terms of encryption, segmentation (due to shared resources), multiple layers of separation, stronger authentication, and better logging and monitoring tools.

Finally, service providers are more likely to have teams of security experts to assess operational risk, as well as risk related to architectural changes.

The UK Government has published Cloud Security Principles providing guidelines to help consumers evaluate cloud services.

Cisco 2017 Midyear Cybersecurity Report

One-third of public sector organisations said that targeted attacks, Advanced Persistent Threats (APTs) and insider exfiltration are high security risks.

In addition, public sector security professionals said that public cloud storage and cloud infrastructure are the most challenging elements to defend against attacks.

Access the report here

[3]IDC "Assessing the Risk: Yes, the Cloud Can Be More Secure Than Your On-Premises Environment", July 2015

2: Data sovereignty and compliance

It is imperative for any organisation to comply with data protection and privacy regulation. Although 'compliance' is a broad term, in general, regulation in this area is concerned with assuring the Confidentiality, Integrity and Availability (CIA) of data.

Through frameworks such as G-Cloud, public sector organisations can access a wide range of cloud offerings provided by service providers.
These offer different levels of assurance, accreditations and SLAs, and are designed to be compliant.

However, many public sector organisations are concerned about whether using cloud solutions will breach their compliance with requirements for data sovereignty and offshoring, defined as: "the performance of any part of the services or a solution under a contract may occur outside the UK for domestic (UK) consumption". Offshoring is officially permitted in principle, but according to the HMG's Offshoring Policy, public sector organisations need to consider whether offshoring is "safe, legal, sensible, the right solution for their business, and the best value for money option".

There are **two pathways** for approval regarding offshoring:

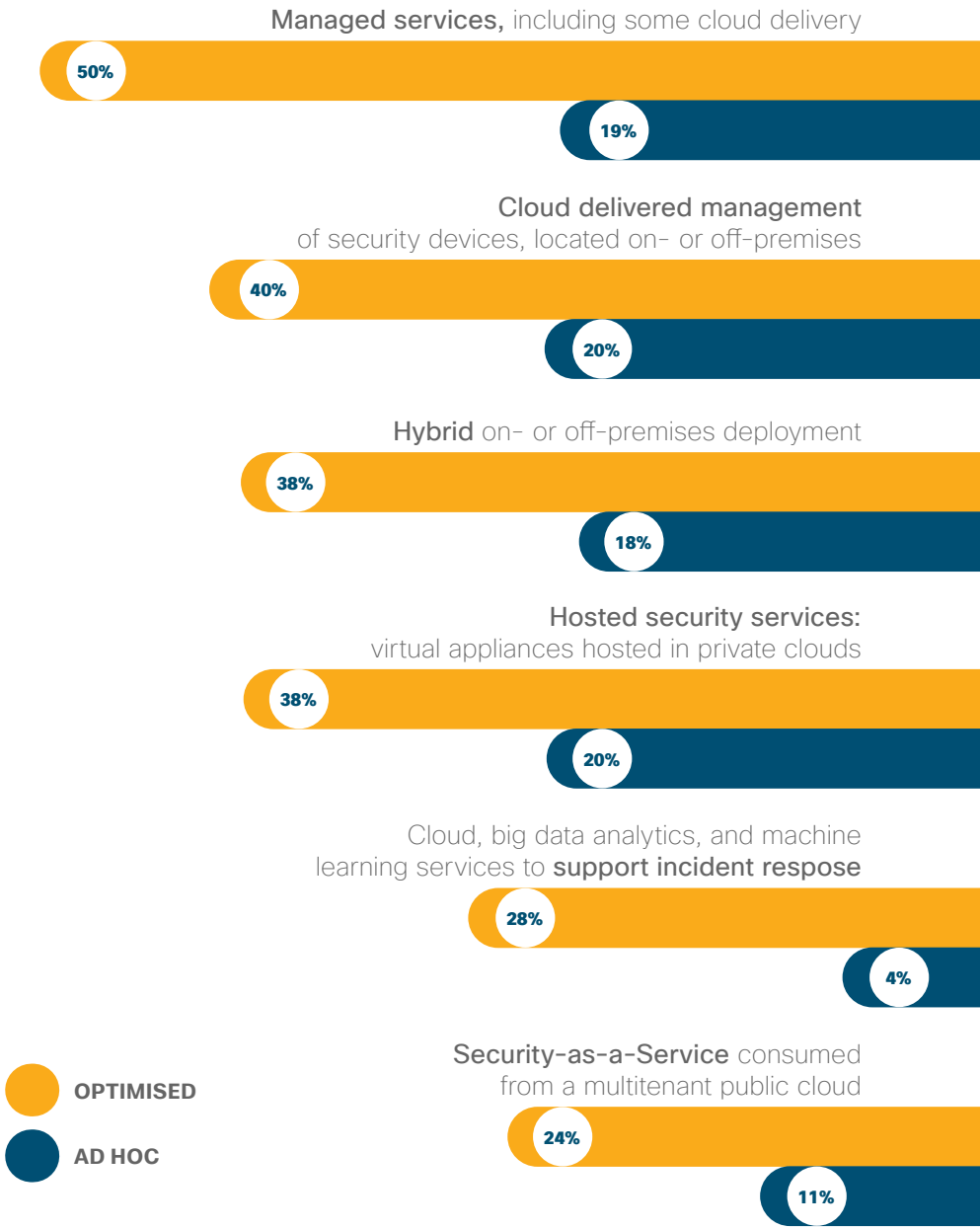
- **Pathway 1** relates to offshoring within countries considered appropriate within the EEA and departmental Senior Information Risk Officer's approval is required.
- **Pathway 2** relates to offshoring within countries outside of the EEA and departmental Office of the Government Senior Information Risk Officer (OGSIRO) approval is required.

Irrespective of type of solution employed, the buyer and supplier share responsibility both for regulatory compliance and policies such as the UK Government Security Classifications (April 2014) and data protection legislation (e.g. DPA, 1998 and GDPR, 2018).

There is an Offshoring Tool to help with the approval process. Meanwhile, the Information Commissioner's Office (ICO) has published relevant guidance for both the General Data Protection Regulation (GDPR) and Cloud Computing.

Figure 2:

METHOD OF CONSUMING SECURITY IN CLOUD ENVIRONMENTS



n = 1,506
Source: Cisco-sponsored Business Value Extension to IDC's Cloudview Survey, 2016

3: Vendor lock-in

The multicloud world that has emerged offers a wide range of services. The public sector has a wealth of opportunity to prioritise business requirements and desired outcomes over technology stacks and infrastructure investment.

While investing in different clouds by definition decreases the risk of vendor lock-in (more clouds, less lock-in per cloud), it is still an area of consideration. And although the commitment' and associated opportunity risk of selecting a specific SaaS offer might be clear, it may be less obvious as far as platform (PaaS) and infrastructure (IaaS) solutions are concerned – which often promise portability options.

In reality, moving data and applications from one provider to another or between a public cloud and an on-premises environment can prove complex due to incompatible data formats, potential network bandwidth costs for egress, and proprietary platform development APIs. There can also be inconsistencies in performance when moving virtualised workloads to platforms based on different infrastructure.

Cloud native applications, based on microservices, can increase the risk of vendor lock-due to API dependencies within the proprietary PaaS environment.

The use of container solutions (e.g. Docker) can improve application portability, but doesn't necessarily solve the issue.

4: Shortage of cloud skillsets

Cloud computing can introduce a host of additional technologies for IT teams to contend with. As organisations build new cloud stacks that offer a new layer of automation, there is often a lack of skills from an operations perspective. DevOps is a good case in point.

Typically, the “Ops” part of the DevOps equation is focused on maintaining and automating the infrastructure (on-premises or Public Cloud resources and tools) for developers to deploy code. Developer teams should be focused on delivering new functionality in an agile methodology without having to worry about the underlying mechanics. However, traditional infrastructure and operations teams lack these skills.

As a result, it is the ‘cloud infrastructure’ piece where the skills gap exists. Organisations need to invest in acquiring these skills, in many cases by enabling Infrastructure and Operations teams. A good starting point is to approach cloud not as a technological shift, but rather a methodology that unlocks capabilities and drives (and requires) business transformation.

Applying a culture where automation and agile provisioning of technology resources spans across teams and not silos is a fundamental ingredient to adopting cloud. In order to drive this from an organisational viewpoint, effective change management is vital. But this can be challenging when there is limited or zero open headcount. Organising workshops to revamp processes and kick-start a new culture is difficult when employees have their ‘day jobs to attend to.

Working with a specialist service provider not only helps a public sector organisation to set strategy and define processes, but also assists with technology transitions during migration and integration. It helps with the day-to-day running of new services, either during a knowledge-transfer period or on an ongoing basis as an out-tasking or managed services arrangement. Finally, it brings a valuable outside perspective on the potentially tangled organisational issues, accelerating outcomes.

While public architecture skills and technical expertise are the most obvious requirements when adopting cloud, ‘big picture’ thinking that leads to business-driven service design and improved technology alignment should be equally prioritised.

Elevate your experience for a multicloud world

Central government policy has made it clear that cloud native is a central pillar of its digital strategy. One that creates a secure, open environment for delivering the next generation of services for citizens and businesses.

There is substantial evidence showing that those organisations who are more mature in their use of cloud reap greater benefit irrespective of the perceived challenges – whether skills, compliance, vendor lock-in, or security.

To realise their aspirations and truly benefit from the opportunities in this new cloud reality, public sector organisations must evolve through a unique journey of transformation in several stages.

Becoming cloud native is not something that can happen overnight, or indeed, with the flip of a switch. It will require understanding and analysing the starting point of this transition, while setting realistic objectives and KPIs at each stage.

The multicloud world allows for applications and business functions to be the starting point for this transition, driving the evolution of public sector infrastructure and networks, spanning multiple clouds and offering advanced security, intelligence and an enhanced user experience.

Cisco's vision for every infrastructure and network is exactly this: a secure platform for digital business.

Find out more about Cisco's cloud vision or call 08004047778.