Bringing Cloud Clarity to Public Sector Organisations

‘Cloud Confusion’ is Hindering the Adoption of Cloud Services in Public Sector Organisation

Just over three years ago, the UK Government launched its ‘Cloud First’ initiative. Today, around 24% of departments still don’t use the cloud, according to a poll of senior decision makers. When cloud can improve efficiency and security, save costs and help with the digital transformation of the UK’s public services, why is it not more widespread? There are a number of myths around adoption of cloud which need to be debunked. The ‘Cloud Confusion’ that’s hindering takeup can only be cleared by a step-by-step analysis of the facts. This white paper highlights these and shines a light on some of the challenges faced by organisations embarking on a cloud journey.

24% of departments still don’t use the cloud, according to a poll of senior decision makers

There is sound reasoning behind moving to the cloud. It not only helps reduce IT spend, but can transform the way an organisation works.

It can offer:

- **Faster, more agile hosting** – allowing service owners to keep pace with development demands
- **Cost effectiveness** – delivering capital and operational cost savings
- **Stronger security** – more secure than the traditional data centre
- **Lower risk** – eliminates dependence on ageing infrastructure
- **Agility** – solutions can quickly and easily flex and adapt as requirements evolve.

If you haven’t already made the move to the cloud, hopefully some of the points and tips in this paper will help highlight some of the key benefits and expose some of the inaccuracies regarding cloud migration.

The Changing Landscape

The number of public sector-focused cloud providers has grown significantly since the introduction of G-Cloud. At first, cloud providers wanting to sell their offerings via G-Cloud were required to obtain Pan Government Accreditation (PGA) against a challenging Impact Level (IL) assessment. This resulted in only a small number of providers accredited to provide cloud hosting services to Government.

2014

'Cloud First' initiative launched by UK Government

The new **Government Security Classification** policy came into effect as of April 2014 changing how information assets are classifed and protected, which has resulted in just three levels of classification (OFFICIAL, SECRET and TOP LEVEL). Closely following the information marking change was the announcement that suppliers no longer needed to undergo Pan Government Accreditation to list their cloud services on G-Cloud. Instead, all cloud suppliers were required to self-assess their services. This has put the onus for selecting the most appropriate cloud services on to buyers, who now face a greater and more confusing roster of cloud providers, including large providers such as Amazon Web Services (AWS) and Microsoft Azure.

This is a fundamental shift, and while it means there is more choice on the market, over 25% of respondents still believe that they must pick an IL-accredited provider. This highlights that many departments still aren't aware of the impact of Pan Government Accreditations ending.

The range of cloud maturity between different departments is striking. Of the 76% that currently use cloud services, most use a single provider, while others have adopted multiple cloud providers. 48% of those surveyed mentioned they would choose a hybrid cloud model if they were building an IT infrastructure from scratch. Every platform has its own nuances and there is a need for more information sharing to help identify which hosting platform or service provider represents the best option.

Kainos recently worked with the Driver and Vehicle Standards Agency (DVSA) to deliver an online, digital MOT service which followed the 'cloud first' approach mandated by GDS. DVSA made the decision to move its cloud services to AWS, enabling it to achieve increased performance and flexibility and ultimately giving it the infrastructure it needed to move forwards with its digital transformation.

76% of Government departments surveyed have some form of cloud solution in place

48% of those surveyed mentioned they would choose a hybrid cloud model when starting a new project

Bringing Clarity

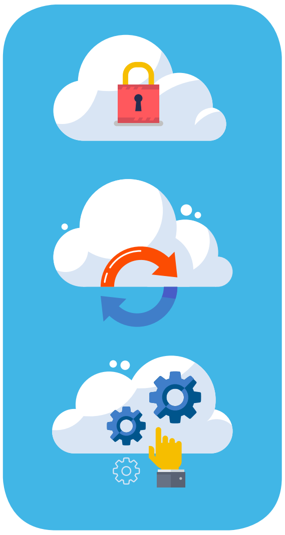
When polled, 80% of Government IT decision makers expressed a strong opinion that the cloud is a good idea, and that more departments should adopt cloud-based solutions. However, despite the desire to change, there are barriers – and over 90% of respondents highlighted the need for some kind of help to overcome these.

Most of you will have determined that your next IT step will be further into cloud, but how to go about doing this isn't always clear.

90%

of respondents highlighted that their department would need help in implementing a cloud strategy

Recent research conducted by Kainos highlights the top three user concerns of moving to the cloud are:



Security

How to migrate data

Picking the right cloud provider

Security

Security is the biggest operational challenge for public sector organisations in moving to the cloud.

> “It’s very easy to focus on functionality and cost savings – but if you compromise on security, the results could be disastrous.”

Of those who have moved to the cloud, 53% cited getting the security right as the greatest challenge. Only 8% of those surveyed still think that the risks outweigh the benefits – so views are changing and people know that security is improving. This tallies with recent research by Gartner, which suggests that in two years’ time, the security benefits of cloud computing will outweigh cost benefits as the main driver for Government agencies to move to the cloud.

53% of Government departments still think security is the biggest issue when migrating data to the cloud

8% of respondents still think that the risks of moving to the cloud outweigh the benefits

Some cloud services like AWS and Microsoft Azure can be set up by anyone with a credit card. Such ‘consumer’ access to cloud - and keeping it separate from Government/citizen data - is a key element of the CESG cloud security principles. Government departments must ensure that there is a separation between consumer and Government data – but how do cloud providers guarantee it? Anyone could be doing malicious things on those services. That’s why some people have chosen public sector-only providers like Skyscape. It’s vital to have a technical conversation with independent experts to find out how providers will segregate tenants on their platforms and thus secure your data.

One key thing to remember is that operational security applies to both the consumer and provider. People assume they are buying a secure service, and generally they are. But too many assume that it stays that way indefinitely. When you start to build on top of the standard service, it can make the solution insecure. Cloud providers give you a set of building blocks – and you can use them to build robust and secure platforms. There is also the possibility that those building blocks are used incorrectly, resulting in operational and security risk. 52% of departments surveyed by Kainos said that getting their cloud solution “secure enough” was their biggest worry. Using an independent expert to help develop and build a bespoke solution can help alleviate worries.

52% **of departments surveyed by Kainos said that getting their cloud solution “secure enough” was their biggest worry**

Different providers will offer different levels of service and associated protection. A cloud solutions provider will always protect themselves, but it’s not automatic that they will extend that protection to you. It’s a customer’s responsibility to remain operationally secure. Before the development of cloud solutions, organisations could outsource whole platforms to external providers, who took responsibility for managing the security. Today, the cloud first approach and distributed nature of service management, means it’s down to the customers to take responsibility for their own applications and manage operational security as a result.

Top Tips

- ✓ First ask yourself ‘how secure does the data need to be?’ Match security needs to the data use case and work from there – the Government’s 14 Cloud Security Principles will help.
- ✓ Providers won’t openly tell you how they secure the data, but under an NDA they can give you some further information about security procedures.
- ✓ Assess what a cloud provider is offering you for gaps in their security procedures. You then know what’s up to you to secure.

Migration

One of the big worries around migration to the cloud is losing control. In fact, 44% of IT decision makers in Government believe they don't have a choice over what data they migrate - but they do feel like they have control over that data once it is in the cloud.

44% **of IT decision makers in government believe they don't have a choice over what data they migrate**

The 90/10 rule is a good one in the case of cloud migration. About 10% of data is highly sensitive and can't be stored in the cloud, but the other 90% is fine to be migrated. The biggest challenge for many departments is differentiating between those two sets of data.

90/10 Rule

90% **of data is safe to be migrated**

10% **of data is highly sensitive and can't be stored in the cloud**

What often happens is that people over-classify the sensitivity of their data. This is sometimes because it's so entwined that it's hard to classify correctly. At other times, it can be the case that the sensitivity of the data is mis-classified against a department's guidelines. There needs to be a greater separation between sensitive and regular data to allow for simpler cloud migration without compromising data security. In addition, that data needs to be stored in a way that can be differentiated.

In some cases, data cleansing will help. A clean data pool will reduce hosting costs and simplify management in any case. Redundant, Obsolete and Trivial (ROT) data is unstructured data scattered through an organisation which has no business value but clogs up and slows down systems, for example email duplicates, video files and terminated employee documents. Make sure you remove all ROT data before migrating, to ensure that relevant data can easily be searched for and found in the cloud.

One important difference between Government departments are the regulations on where data can be stored. Some departments must keep data within very specific geographic areas. For example, NHS patient record data is not allowed to leave the borders of England, sometimes it cannot be stored outside Trust boundaries. Other departments are less specific and allow storage in the UK or in EU countries.

For most Government organisations, storage in the UK is the rule, but there's a lot of variance. It's down to the Information Assurance team to get to the bottom of the regulations and confirm where data needs to be hosted.

85%

of data held by organisations is redundant, obsolete and trivial and therefore creates costs

Top Tips

- ✓ Encourage your Information Assurance teams to consult with CESG for guidance, especially with regards to rules and regulations on data hosting.
- ✓ Be ruthless in your decluttering. 85% of data held by organisations is ROT and therefore creates costs. Clean data properly before migrating and costs could reduce dramatically.
- ✓ Clearly assess data against specific criteria. There is often a tendency to over-classify data security classification, which in-turn makes it hard to determine what data can be migrated to the cloud.
- ✓ Check the storage requirements of your data – both geographically and security-wise. There are some stringent rules on where data can be hosted, but they're not the same for everyone.

Choosing a Provider

Doing research to whittle down a list of providers based on what your requirements are is often easier said than done. This includes the infrastructure, the location of where the data needs to be stored, and core capabilities.

20% of those surveyed said they don't know where to start, or which provider to use

Picking a provider is still a big challenge for departments – over 20% of those surveyed said they don't know where to start, or which provider to use.

When it comes to picking a provider, ask the shortlisted suppliers to clarify aspects of their service that need to align with your specific needs. That should then be followed up with a face-to-face meeting so you can confirm specific details. Be selective about your selection criteria: if you focus on peripheral requirements, the provider that can meet all demands may not be able to address the most important elements. Clearly, the selection process has to be fair, regardless of whether you have a preference for one provider over the other. If two providers are exactly the same on paper, then the government procurement process will guide you towards the cheapest provider.

Align provider's services with your specific needs

Face-to-face meeting with the provider

Be stringent about your selection criteria

It's important to pick a provider that can meet the scale and demand of your services. Departments tend to dip their toe in the water and start with a smaller provider. However, they then often find that they have not adopted the new solution in a way that scales both technically and operationally. **There's a reason people mix and match cloud providers, but it's important to speak to an expert if you're looking to use multiple cloud providers to ensure you've got the best mix for your department and the best solution for both your long and short term needs.**

It's important not to compromise on your 'must-have' requirements, so be definite on what they are. Use your "future needs" requests as an opportunity for providers to differentiate themselves. This will eliminate some of the more short-term thinking providers. Most contracts are two years long – but don't panic if you realise within that two-year period that the solution is no longer right for your needs. Most providers also have a one-month notice system in place, so you can change providers or adapt your contract more frequently.

18% of departments polled noted that their next step on the cloud journey is cloud-to-cloud migration

This shows that moving from one provider to another is not the daunting task it once was.

To help set the groundwork for migration to a different platform in the future, make an assessment of set-up costs versus future migration costs. That means, for instance, deciding whether to design your own load balancer, or use the vendor's native one. It will cost more in the short-term, but allow you to move more easily in the future. What provides the best value? Of course, migrating later is not impossible, but you can protect yourself against some of the costs now by being selective in how you structure your new agreement.

When looking at scale, you really need to focus on the volume of transactions. For example, the DVSA manages over 150,000 MOT tests a day by 69,000 testers, across 22,000 garages, so it has a high volume of transactions. Others are lower, and don't need the same level of scale. It's important to share your requirements for scaling solutions up front. There are some providers who are more comfortable with handling huge volumes of transactions, whereas some of the smaller providers will be unable to scale on the same level.

Top Tips

✓ Keep an open mind. It is a rapidly developing industry and the providers you've worked with before may not be the best choice.

✓ Speak to an independent expert, especially if you're looking to use multiple cloud providers. 54% of departments surveyed by Kainos mentioned that they would need external help in picking and building a cloud solution.

✓ You can change provider if you're not happy. Before entering a contract, make the right architectural decisions to make sure you don't get locked in.

Conclusion

Speed of deployment, flexibility and reductions in cost are just a few of the many benefits of cloud computing in the public sector. There are many barriers standing in the way of migrating to the cloud, but all can be overcome with the right support.

The key problems that IT departments worry about don't have to get in the way of migrating data to the cloud. Segmenting data, interrogating storage and security regulations and future-proofing in-house are central elements. The enabling factor is finding a partner that can help share experience of these kinds of projects and knowledge of the marketplace.

The process certainly isn't simple, but with the right independent advice from experienced practitioners, migration to the cloud can become manageable and rewarding.

Get started on your cloud journey

Cloud Services
kainos.com/cloudservices

Contact Us

twitter.com/KainosSoftware

linkedin.com/company/kainos

cloudservices@kainos.com

kainos®

About Kainos

Kainos is a trusted partner for UK Government, leading the digital transformation of public services by delivering smarter, faster, better solutions.

We've over 30 years of experience and have played a central role in more than 40 Government digital projects. Millions of UK citizens are already benefiting from the public services we have made digital by default, and simpler to use.

We deliver innovative and evolving solutions that exceed expectations, and that are secure, accessible, and cost-effective. We work collaboratively with departments to shape projects and build digital capability through a full portfolio of services, including: agile delivery, digital consulting, cloud and data services.

At Kainos we have a highly skilled and motivated team of over **800 people** and are recognised as **digital leaders** in UK Government.

kainos.com