Addressing the 12 blockers to IT modernisation with a multi-cloud strategy

ukcloud

CONTENTS

INTRODUCTION

In February 2020, UKCloud in partnership with Censuswide, surveyed more than 300 IT professionals and business leaders from a variety of public sector organisations, large and small, up and down the country to determine the State of Cloud Adoption in the UK public sector.

The results were emphatic. There is clear desire to adopt cloud[1] and cloud is broadly recognised as a key enabler[2] to harness other digital technologies like artificial intelligence, sensor networks (IoT) and robotic process automation to deliver better outcomes to users of public services.

So, what is holding back greater adoption of cloud? The survey revealed a number of technical and non-technical challenges. Challenges that confirm that there can never be a single public cloud that is best suited to all the requirements that an organisation will have. Indeed, Red Hat said it well,

> **"You might find the perfect cloud solution for one aspect of your enterprise — a proprietary cloud fine-tuned for hosting a proprietary app, an affordable cloud perfect for archiving public records, a cloud that scales broadly for hosting systems with highly variable use rates — but no single cloud can do everything (or, rather, no single cloud can do everything well)".**

Hence, the current focus on the global cloud wars (AWS versus Azure versus Google) is at the heart of the problem. These cloud providers are certainly part of the solution — but the answer requires a combination of different cloud platforms. Rather than placing a big bet on the single best public cloud, organisations must adopt a multi-cloud strategy in order to address the diversity of their requirements; now and into the future.

In fact, the survey found strong support for multi-cloud[3] and that less than one-in-five[4] respondents believed all their requirements could be met by a single public cloud.

This e-book explores the 12 key issues and concerns (blockers) raised by public sector organisations that inhibit the modernisation of their existing and legacy environments and explains how multi-cloud solutions can best bridge the gap between 'actual' and 'aspiration'.

1. 87% agreed "If one perfect solution existed, I would move all of my IT to the cloud"
2. 81% agreed "Cloud is merely an enabler for my organisation to adopt transformative technologies like Artificial Intelligence, Smart Places and IoT/hyper-connectivity"
3. 86% agreed "I would prefer to have a multi-cloud vendor"
4. 19% agreed "We will only use a single Public Cloud"

CHAPTER 1

ADDRESSING THE COMMERCIAL RISKS OF CLOUD ADOPTION

In this chapter, we'll start with some of the key non-technical blockers to cloud adoption that cause organisations to rightly question where they're heading and the consequences of becoming over-dependent on a technology or provider.

1

BLOCKER 1: CONCENTRATION RISK

The survey echoed growing concern about the risks of becoming dependent on the services of a single cloud platform. A large majority of respondents expressed a concern about 'concentration risk' and having all their eggs in a single basket. This could be due to the 'Carillion effect', the heightened awareness across public sector of the severe implications on the delivery of public services should a provider fail or encounter difficulties. It is easy to imagine the potential consequences on public services should one of the global cloud providers encounter service issues or decide to redistribute their resources across other datacentres outside of the UK.

Further, organisations such as the Bank of England and European Banking Authority (EBA) have considered the potential negative impact to the financial services sector should a leading cloud provider, which has become 'too big to fail', actually fails. Recently, the European Union has explored this problem which has led to the announcement of Gaia-X and a commitment by EU member states to manage the level of dependency on global clouds by having their own national clouds.

Once again, most survey respondents cited concerns over risks and security as an inhibitor of cloud adoption. And when it comes to the concern as regards concentration risk, the ability to spread commercial risk across multiple technologies and providers is one of the clearest drivers of a multi-cloud strategy.

ACTION PLAN:

- **LEARN:** about the National Audit Office's and European Banking Agency view of concentration risk and why it is essential to avoid it
- **PLAN:** Run a discovery exercise to determine where all of your applications and datasets are hosted, including SaaS applications and shadow IT
- **ACT:** Track concentration risk as a business risk at board level to ensure that you are regularly reviewing the level of exposure you have to a single provider

As multi-cloud experts, UKCloud provides a range of cloud agnostic advisory services that help organisations determine the ideal mix of different cloud technologies and cloud providers. This ensures organisations don't inadvertently become over-dependent on a single provider.

2

BLOCKER 2: VENDOR LOCK-IN

Concentration risk is closely related to the risk of vendor lock-in, by exploiting technical features that are unique to that provider and would result in the application needing to be rewritten or heavily modified to be moved. Organisations that are locked-in can be held to ransom by the vendor through higher support costs and/or lower service levels and the inability to move because the cost of rewriting the application is prohibitive. Nearly three-quarters of respondents declared that they had been subject to vendor lock-in in the past.

Typically, vendor lock-in occurs as a specific layer of the stack — the application layer such as Oracle or SAP, the operating system layer such as Solaris or Windows, or the hypervisor layer such as VMware. Traditionally, lock-in at one layer, still provided some choice at other layers — e.g. choice of hosting location, choice of infrastructure vendor, etc. However, global cloud lock-in is deeper — not only can lock-in occur due to proprietary platform / APIs, but lock-in also inherently occurs through the stack — the infrastructure vendor, the hosting location / datacentre. It is therefore not surprising that respondents expressed a clear fear of vendor lock-in.

Analysts such as Gartner have also commented on this concern, "Most organizations adopt a multicloud strategy out of a desire to avoid vendor lock-in or to take advantage of best-of-breed solutions. The decision may be driven by a variety of factors, including availability, performance, data sovereignty, regulatory requirements and labour costs."

ACTION PLAN:

- **LEARN:** Understand why analysts and commentators advocate a multi-cloud strategy
- **PLAN:** Implement governance through your Technical Design Authority such that business cases advocating the use of proprietary cloud features must be signed off by the CIO
- **ACT:** Conduct a cloud assessment to create an actionable plan to migrate services to multiple cloud services

UKCloud's approach to multi-cloud tackles that head on. Organisations can run the cloud at the location of their choice; on-premises, 3rd party data centre, Crown Campus or global cloud data centres. And organisations can mix-and-match the cloud technologies of their choice — from VMware to Azure, from Office 365 to OpenShift. With UKCloud, it is all about choice.

CHAPTER 2

ADDRESSING THE FINANCIAL CONCERNS OF CLOUD

Issues related to cost and budgeting were particularly prevalent in the survey responses. Indeed, "Cost / affordability" was the single biggest concern of respondents agreeing this was an inhibitor to cloud adoption and IT modernisation. Whilst total cost of ownership (or affordability) is certainly a concern, it was also interesting to discover nuances in terms of the configuration of the budget (capex/cdel versus opex/rdel) and budget management of consumption based costs versus fixed asset purchases.

3

BLOCKER 3: BUDGETING FOR CAPEX AND OPEX

Most respondents stated that the "Misalignment with organisations budget (CAPEX vs OPEX)" is an inhibitor to cloud adoption. And beyond mere misalignment, nearly half those surveyed said, "We find CAPEX costs easier to budget for than variable OPEX costs".

This creates a major problem when considering a 'public cloud only' strategy as all public clouds are treated as an OPEX cost. For organisations that also have a CAPEX budget, private cloud is the answer as it gives organisations the ability to run on-premises (in its own data centre) as well as Crown Campus. And wherever the private cloud is hosted, organisations have the option to buy the cloud infrastructure as a capital expenditure.

ACTION PLAN:

- **LEARN:** Understand how your organisation prefers to budget for IT spend
- **PLAN:** Determine key milestones such as end of lease for your datacentre, end of enterprise license agreements (ELA), infrastructure refresh cycles as these drive significant CAPEX spend which your organisation might prefer to avoid/reduce
- **ACT:** Understand how different cloud deployment models (public cloud, hosted private cloud, on-premises private cloud) suit your budget

Multi-cloud solutions are the best option for most organisations as it enables each organisation to find the best mix of opex-based public cloud services and capex-based private cloud services in one integrated solution.

4

BLOCKER 4: RUNAWAY VARIABLE COSTS

The second issue relating to costs that was reported by those surveyed is the concern that "the difficult-to-predict variable costs of Public Cloud will lead to cost overruns". This concern is based on the 'hidden' costs of the global cloud platforms such as bandwidth, data IO and even support costs. Indeed, 4 in 5 respondents agreed "Fear of runaway costs hinders buy-in of cloud adoption in the organisation".

This often leads to a common scenario where a cloud project costs are more than originally budgeted because these 'hidden' costs were difficult to predict and control. This drives interest in easier to budget, more cost predictable, cloud solutions such as private clouds, or public clouds (such as UKCloud) that have a simpler pricing model whereby bandwidth, data IO and support costs are not charged separately.

For example, during a recent webinar on budgeting and affordability, Shaun Collings, Director - UK Public Sector at Pure Storage advised, "A lot of folk are looking at backup to cloud but I would suggest that folk don't just look at the backup, but also look at the restore from cloud" as the restore from global cloud platforms will incur data egress bandwidth costs that can make the solution cost prohibitive.

ACTION PLAN:

- **LEARN:** Evaluate the pricing model of your cloud service — beyond the headline 'per instance' price, how are components like bandwidth, IO and support packaged in the context of a real use-case?
- **PLAN:** Ensure you have a plan to reduce your commercial exposure to a single cloud platform by having appropriate governance on which services are allowed to be consumed
- **ACT:** Perform a cloud optimisation cost assessment to better understand the costs of your current cloud services and how they can be optimised

This concern has become so common that solutions such as VMware CloudHealth specialise in analysing the costs of public cloud platforms. UKCloud's Cost Optimisation Service uses VMware CloudHealth to help organisations take back control of their public cloud costs — which in some cases results in repatriating workloads from global cloud platforms onto other multi-cloud platforms including private cloud.

5

BLOCKER 5: AFFORDABILITY

The survey also found a significant concern related to the overall cost relative to traditional solutions. More than half those surveyed "believe cloud is more expensive than on-premises for traditional applications".

These challenges are certainly applicable to global cloud platforms which are designed for elastic and dynamic workloads that only use underlying resources when needed. Traditional applications are designed to scale-up rather than scale-out and tend to consume a minimum footprint 24/7 regardless of actual demand on the application. Hence, these are a poor fit for global cloud platforms and those who have tried to migrate these applications have soon realised that the costs can be unsustainable. Contrast this with private cloud environments which are much better suited to these types of usage profiles often making private cloud solutions directly comparative to traditional on-premises environments.

Almost a third of those surveyed said, "we can't afford to adopt cloud until our existing IT investments are fully depreciated". The nature of capital expenditure creates the lock-in to depreciation cycles. The business case for a capital expenditure typically looks at the total cost of ownership over a 3-7 year period. To get the desired return on investment, the assets are expected to be fully utilised throughout this period. Hence, organisations that are considering a cloud migration will often be challenged by the finance team because doing so would result in assets that haven't been fully written down.

ACTION PLAN:

- **LEARN:** Explore the wider cloud marketplace by looking into specialist cloud providers that are present within the government's Crown Campus
- **PLAN:** Broaden your cloud strategy to consider how to modernise your existing and traditional applications by using multiple cloud solutions that are connected to your existing systems
- **ACT:** Conduct a cost optimisation assessment to better understand the extent of cost overruns on the global cloud platforms

UKCloud can help with these challenges in various ways. Multi-cloud enables organisations to mix-and-match private clouds and public clouds for the most optimum and affordable solution. We also work with vendors, such as VMware, to review existing Enterprise License Agreements (which are usually capitalised) in order to determine whether these can be switched to a Cloud Adoption License Service — essentially replacing a fixed cost, fixed term license agreement with one which can scale-up and scale-down as the configuration of the existing environment changes. And because we operate within with Crown Campus, there is the potential to physically 'lift and shift' existing assets into Crown Hosting so that they enjoy physical adjacency with our multi-cloud platform.

CHAPTER 3

ADDRESSING THE SECURITY AND ASSURANCE CHALLENGES OF IT MODERNISATION

It is no surprise that risk and security was one of the most common inhibitors to IT modernisation and cloud adoption, with 85% of those surveyed agreeing that, “My organisation is reluctant to move workloads to the cloud due to risk and security concerns”. This chapter explores few dimensions to this.

BLOCKER 6: SECURE AND SENSITIVE SYSTEMS

Almost half those surveyed stated that they wouldn't consider public cloud for "My most secure and sensitive systems". This certainly includes those systems that have a higher classification level such as SECRET, but it also includes a large number of traditional environments that act as the System of Record and underpin the core public services that are delivered by the public sector organisation. These organisations rightly prefer more control over these systems and are less willing to take risks with them.

Nearly half the respondents agreed they wouldn't consider public cloud services for "Systems that need to run on-premises or in Crown Hosting". It is often accepted that cloud platforms can be more secure than on-premises, but with the global cloud platforms many of the security controls are options that add costs and complexity to the solution relative to more traditional approaches to on-premises environments.

The government recognises that on-premises datacentres and computer rooms are often not sustainable as they are expensive, inefficient and often lack resilience. Hence, the government launched the Crown Campus from Crown Hosting Datacentres which is a joint venture between the Cabinet Office and Ark Datacentres and designed to provide a secure, sustainable and affordable UK sovereign datacentre facility — especially for the nation's most secure and sensitive systems.

ACTION PLAN:

- **LEARN:** Understand how the government's Crown Campus is designed for the nation's most secure and sensitive public services
- **PLAN:** Conduct a discovery workshop to determine how specialist public cloud and private cloud services work alongside global cloud options
- **ACT:** Conduct a proof of value exercise to validate how easy and affordable it is to integrate specialist cloud services into your environment

UKCloud operates from the government-grade Crown Campus which is optimised for the most secure and sensitive systems across UK public sector. UKCloud's multi-cloud platform is designed to span multiple classification levels or trust zones. Like all global cloud platforms, the UKCloud Assured OFFICIAL platform is natively connected to the Internet to support population-scale systems. Uniquely, UKCloud offer two further platforms best suited to secure and sensitive environments:

1. **The Elevated OFFICIAL platform is decoupled from the Internet and is considered 'behind the firewall' for many organisations as it connects directly the secure and private networks.**
2. **The Tier 2 platform is suitable for higher classification levels and benefits from enhanced levels of assurance across the people, processes and premises.**

7

BLOCKER 7: TRADITIONAL SYSTEMS

Cloud is certainly secure for systems and applications that have been designed for cloud, as those systems will have several security enforcing controls baked in — from encryption and authentication to continuous deployment of new and updated code.

In contrast, many traditional IT environments were designed to operate in traditional datacentre environment — isolated from public networks like the Internet and accessed only by secure end-points and vetted users. Hence, it is no surprise that nearly half the survey respondents agreed that they wouldn't use public cloud services for "Traditional IT environments that are not cloud native".

It is much more complex and expensive to try and retrofit additional security controls to existing applications. Rather, it would be ideal if one could simply move those systems to a cloud environment that closely matches the characteristics of traditional datacentre environments. Although global clouds do not provide this capability, multi-cloud does provide choice of cloud technology, deployment model (e.g. private cloud) and classification level (e.g. secure cloud).

ACTION PLAN:

- **LEARN:** Understand the key differences between cloud native architectures and traditional application architectures
- **PLAN:** Conduct as assessment and discovery to identify your existing applications and determine how each one of them fits into a multi-cloud strategy
- **ACT:** Download a 'free trial' from UKCloud to enable your teams to experience how familiar the VMware Cloud is to your existing VMware environments

Multi-cloud addresses this challenge. Multi-cloud brings together public cloud platforms which are great for cloud native applications, with cloud technologies such as Oracle and VMware or private cloud deployments that more closely mirror traditional architectures. Combined with the Crown Campus, you'll be able to create hybrid environments spanning physical servers, virtual services, containers and cloud.

BLOCKER 8: ACCESS TO SECURE COMMUNITIES

More than a third of respondents said that they wouldn't use public cloud services for "Systems that need to connect to private or community networks (like PSN, HSCN and RLI)" in order to be accessible to communities of vetted users (such as health professionals and intelligence officers) or to connect to legacy systems — commonly systems of record which aggregate large volumes of sensitive data.

The challenge is that global cloud platforms are designed to connect natively to the internet. It becomes complex and expensive to implement the architectures necessary to securely connect these global clouds to secure or private public sector networks. Moreover, the controls required go beyond merely technical components like encryption. Most secure networks require specific assurances related to people (e.g. vetting and security clearance), processes (e.g. code of connection) and premises (e.g. secure hosting of network termination equipment). Hence, most customers consider cloud only for new applications designed to be delivered over open networks such as the Internet.

Further, the requirement for lockdown and social distancing in response to the COVID-19 pandemic highlighted the need for secure and compliant remote access to secure networks and systems. Providers like UKCloud offer secure remote working solutions based on 'walled garden' architectures aligned with NCSC good practice which facilitate the secure and controlled sharing of information between higher security domains and lower security domains (such as work from home environments).

ACTION PLAN:

- **LEARN:** Review the systems and users connected to your private and secure networks
- **PLAN:** Request a discovery workshop to better understand how UKCloud's connectivity options create new possibilities for your multi-cloud strategy
- **ACT:** Conduct a Data Assessment Service from UKCloud to review where your important datasets are situated

UKCloud's multi-classification platform is designed to natively connect with these secure community networks or private networks. Organisations often consider the UKCloud platform as an extension of their internal network (i.e. behind their firewall just like your existing datacentre environments) and so provides a safe and trusted alternative to public cloud. Further, public sector organisations are increasingly using Crown Hosting for traditional systems that need to connect to secure systems and networks — so UKCloud's prominent presence in the Crown Campus enables those organisations to create secure hybrid environments — connecting legacy (non-cloud) systems to UKCloud's multi-cloud platform which can the extend onto global cloud platforms where appropriate.

CHAPTER 4

ADDRESSING THE COMPATIBILITY GAP BETWEEN TRADITIONAL AND CLOUD NATIVE ARCHITECTURES

There are two sides to the digital transformation that is happening across the UK public sector. On one hand is the creation of new digital services powered by cloud native applications which are designed to operate in the cloud. On the other hand is the vast number of existing and traditional IT environments which exist on-premises or on traditional data centres. These systems were not designed to operate on the global cloud platforms and so a gap exists between the 'old' and the 'new'. This chapter explores how multi-cloud helps to bridge that gap.

9

BLOCKER 9: APPLICATIONS THAT WERE NOT DESIGNED FOR CLOUD

More than three-quarters of those surveyed agreed that "incompatible applications (not cloud native)" were impeding their cloud adoption. Global public cloud platforms are designed for cloud native applications that were designed and built to operate in a specific way using architectures like microservices, NoSQL, service mesh and similar. However, every public sector organisation has hundreds of applications that were designed to operate in traditional environments. Many of these applications can be made to run on the global cloud platforms, but because these applications don't leverage the elasticity of cloud, they become very expensive to run and expose potential security vulnerabilities.

In contrast to global cloud platforms, specialist cloud platforms are optimised for traditional applications and so they don't incur this cost premium or potential security issues. Indeed, in many cases, specialist public clouds or private clouds can be less expensive than on-premises environments which addresses a concern that more than half those surveyed expressed that global clouds are more expensive than on-premises for traditional applications.

ACTION PLAN:

- **LEARN:** Understand the differences between specialist clouds like VMware Cloud and global cloud like Microsoft Azure
- **PLAN:** Conduct as assessment and discovery to identify your existing applications and determine how each one of them fits into a multi-cloud strategy
- **ACT:** Use a 'free trial' from UKCloud to enable your teams to experience how familiar the VMware Cloud is to your existing VMware environments

A multi-cloud strategy will only use the global clouds for cloud native applications, and will use specialist public and private clouds to meet the needs of traditional applications. For example, VMware Cloud provides the same level of performance, resilience and configurability as traditional VMware based virtual environments. This makes it possible to migrate existing applications as-is, without going through an expensive and potentially risky transformation.

10

BLOCKER 10: MAINTAINING SYSTEMS THAT CANNOT MOVE TO CLOUD

A third of respondents stated that "Legacy systems such as Mainframe, AS/400 and SPARC" which cannot be run on x86-based cloud platforms, presented a blocker for their cloud adoption. These applications are typically the System of Record in many public sector organisations and so service levels need to be maintained and enhanced — especially as they increasingly need to interface with dynamic digital systems such as Robotic Process Automation or citizen-facing front-end services.

None of the global cloud providers will allow 3rd party environments in their datacentre facilities. So, the options are to keep these systems on-premises, or to consolidate them within the government's Crown Campus — purpose built, secure and energy efficient facilities designed for workloads that cannot move to cloud.

85% of respondents agreed that, "If there were dedicated cloud hosting technologies available that could mirror my existing environment, I would move more workloads to the cloud". The good news is that this is exactly what multi-cloud makes possible — dedicated cloud hosting environments that enable organisations to harness their existing applications, tools and skills in order to acceleration their cloud adoption.

ACTION PLAN:

- **LEARN:** Understand how the government's Crown Campus is designed for public sector solutions that are not ready for global cloud
- **PLAN:** Conduct a discovery workshop to determine how specialist public cloud and private cloud services work alongside global cloud options
- **ACT:** Conduct a proof of value exercise to validate how easy and affordable it is to integrate specialist cloud services into your environment

A multi-cloud strategy enables organisations to embrace non-cloud environments alongside their public cloud and private cloud environments. Cloud providers like UKCloud are based within the Crown Campus and this enables non-cloud and cloud environments to be directly connected with high bandwidth, zero latency and highly secure local connectivity — rather than via wide area network connections. This proximity not only enables co-existence and interoperability between non-cloud and cloud, it also facilitates the transition of services from non-cloud to newly deployed cloud-based services.

CHAPTER 5

ADDRESSING THE SKILLS AND CAPABILITY GAP

Much like the compatibility gap that we explored in chapter 4, there is also a gap between the skills required to operate traditional IT systems and the skills required to develop and operate cloud native systems. Traditional IT systems tend to be based on proven technology products such as SANs (Storage Area Networks), failover clusters, virtualisation and layered security. These systems tend to be operated using established ITIL (IT Service Management) processes. Cloud native systems are different. They require skills relating to automation, Agile, continuous deployment, DevOps and APIs. This chapter explores how organisations can address the gap between traditional IT and cloud native.

11

BLOCKER 11: UNSUSTAINABLE DEVOPS COSTS

Almost 4 in 5 of those surveyed agreed that they lacked the cloud native skills such as DevOps and automation to replace existing applications with cloud-based versions. This should not be much of a surprise as Digital Transformation is a global trend, affecting many industries — not just public sector. Hence, there is significant demand for these skills and not enough supply. Not only does the scarcity of these skills create a blocker for cloud adoption, but it also means that these skills are particularly expensive. People with these skills tend to command lucrative contract rates which many public sector organisations struggle to afford. And we're aware of situations where existing people have been given the training only to leave for the alluring contract market.

Whilst it is true that some of the global cloud providers put particular emphasis on building applications for their cloud, a multi-cloud strategy brings Software-as-a-Service (SaaS) cloud options to the table which enables organisations to seriously consider whether they should be building applications or buying SaaS based alternatives. In our option, there are plenty of specialist SaaS providers that make it cheaper, easier and faster for public sector organisations to achieve the desired outcomes from cloud-based software.

ACTION PLAN:

- **LEARN:** Research the specialist Software-as-a-Service alternatives to your existing applications
- **PLAN:** Review your existing applications to identify which license agreements will soon need to be renewed (or replaced with SaaS alternatives)
- **ACT:** Formalise a policy to prefer buying SaaS over custom developing your own applications

This multi-cloud strategy has a secondary benefit — rather than having to recruit or retain staff with skills that are in much demand, they can focus on harnessing the existing skills and capabilities of their team by focusing on modernising the large number of traditional systems on which public sector organisations typically depend. This is supported by the finding from the survey whereby 85% agreed that they would move more workloads to the cloud if they could find cloud hosting technologies that mirror their existing environment — implying that they have amply skills in those technologies.

12

BLOCKER 12: INERTIA CAUSES BY INSUFFICIENT CAPABILITY OR CAPACITY

A more general blocker to greater adoption is the general lack of skills and resource levels needed to meet the various demands of the organisation. 83% of those surveyed agreed that this was one of the key inhibitors to cloud adoption. Indeed, 85% agreed that their organisation understood what was required to move existing workloads to the cloud, yet 79% are struggling to find the right skills to drive that cloud adoption. We think of this as 'capacity' and 'capability'. Some organisations have the capacity (e.g. the right resource levels) but lack the right skills and know-how (capability). Others, have pockets of great capability but simply lack the capacity to execute. And some public sector organisations lack both the capacity and the capability to drive their adoption of cloud.

However, the survey revealed that public sector organisations are wary of IT projects, with almost three-quarters citing a "fear of failure" as hindering broader buy-in of cloud adoption and almost 4 out of 5 reflecting that the "legacy of previous IT project failures" as also inhibiting cloud adoption.

The key here is that rather than working on 'day rates', organisations should seek 'outcome-based' project deliverables. This helps ensure that public sector organisations get genuine value for money rather than long-running programmes that are lucrative to the provider of day-rate services.

ACTION PLAN:

- **LEARN:** Review the skills and resources that you currently have available
- **PLAN:** Take a Discovery Workshop to map your existing skills and resources to a multi-cloud strategy
- **ACT:** Use approved frameworks like Digital Outcomes and Services (DOS) to commission outcome-based project engagements from specialists like UKCloud

This is one of the primary reasons that UKCloud has developed a professional services capability. We now have the skills and resources to help public sector organisations plan and execute projects to accelerate their cloud adoption and digital transformation. All of UKCloud's professional services are delivered as outcome-based projects.

CONCLUSION

In this e-book we've explored 12 issues and challenges that most public sector organisations will face as they seek to modernise their traditional IT environments and adopt cloud-based solutions.

It's clear that there can never be a 'one-size-fits-all' solution to all of these issues, especially given the different characteristics and maturity levels of public sector organisations. Hence, it is unhelpful that people commonly associate the term 'cloud' with the global cloud providers and forget that there are many types of cloud — some of which are specifically designed to address one or more of the 12 issues and challenges that we've highlighted here.

It is essential that all organisations understand the value of a multi-cloud strategy. Multi-cloud can include the global cloud platforms for cloud native use-cases, but it also includes specialist clouds, private clouds and secure clouds to meet the vast number of other use-cases that aren't optimised for global cloud.

Throughout this e-book we've suggested an action plan to address each of the 12 issues and challenges. If we were to summarise that to just three things; we would suggest that you:

1. **LEARN** about multi-cloud, distributed cloud and hybrid cloud and recognise the value of having a cloud strategy that goes beyond merely building new cloud native applications on a global cloud platform
2. **COMMISSION** a discovery workshop to start to understand the existing and traditional systems and datasets that your organisation currently relies on. Use this inventory to validate that you won't have the time, money or risk appetite to re-write or re-platform all of those applications so re-hosting using multi-cloud might be a compelling alternative
3. **START SMALL, BUT START NOW.** Take your very next traditional IT requirement (e.g. additional capacity, technology refresh, contract renewal) and put multi-cloud to the test using that real life use-case.

ukcloud

Additional information about UKCloud can be found at
www.ukcloud.com or by following us on Twitter at @ukcloudltd

web: www.ukcloud.com | **email:** info@ukcloud.com | **tel:** 01252 303 300