SUNGARD®
AVAILABILITY
SERVICES™

WHY IT IS HIGH TIME FOR THE PUBLIC SECTOR TO LET DATA LIVE IN THE CLOUD.

Sungard AS, a knowledgeable and reliable IT partner, explain in detail here why it is high time for the public sector to let data live in the cloud

The benefits of cloud computing are now widely accepted: increased flexibility, improved collaboration, better document control, the ability to scale up or down as needed and avoiding hefty capital expenditure through a subscription-based model. For these reasons and more, cloud computing has been widely adopted throughout the private sector.

Yet despite all the potential benefits – and the UK Government's Cloud First initiative encouraging the public sector to consider the cloud before any other approach – the public sector still lags behind in terms of cloud adoption. According to a survey of 118 public sector organisations, only 21% said they view the use of the cloud infrastructure as a priority[1].

This is hard to understand when you consider the urgency to leverage digital technologies to change the way government delivers public services, making them more integrated and responsive to citizens' needs. As a strategic and an agile enabler for digital transformation, the cloud seems like the logical choice – and a mandatory one for UK central government agencies.

BARRIERS TO CLOUD ADOPTION

So, why is public sector cloud take-up so low? Until now, there have undoubtedly been three huge obstacles to progress:

1. LEGACY IT MIGRATION

The typical government IT environment tends to consist of a mix of legacy systems, hardware and technologies. Some are easier to move to the cloud than others, some are more costly and risky to move, and some bespoke applications will continue to run on legacy infrastructures over the short or long term (even, in some cases, until the end of their lifecycle).

While the goal of government transformation is to make service delivery more cohesive and efficient across the whole public sector, legacy system integrations pose significant challenges.

[1] Digital Transformation: Delivering IT Efficiency, Survey Report of 118 public sector organisations conducted by iGov in collaboration with Sungard AS, 2017

This is borne out by the fact that 69% of survey respondents said difficulty integrating services across platforms and/or infrastructures was a barrier to sharing data, which is key to streamlined service delivery[1].

2. MAINTAINING SECURITY DURING THE TRANSITION

Considering the complex chain of interdependent systems and workloads involved in delivering even one citizen service, it's easy to see how the smallest IT change can be disruptive, causing a ripple effect. Government departments may be understandably concerned that a cloud transition could affect their ability to deliver the 24/7 service citizens expect.

Furthermore, as they begin to share information and 'join the dots' by integrating processes across the agency and departmental boundaries, they may worry that the technology walls coming down will create security gaps, making data vulnerable. This may be why 79% of digital transformation survey respondents cited data and systems security as their highest priority.

3. THE REQUIREMENT FOR UK DATA SOVEREIGNTY

With growing sensitivities following GDPR, government agencies must ensure that public sector workloads comply with strict data sovereignty and privacy regulations, adding another layer of complexity to the already challenging cloud transition.

While the cloud offers the agility to put data where it makes the most sense to reduce latency (time lag) and deliver a more responsive service to citizens, data sovereignty regulations dictate where the data resides and who can manage it. Now, public sector data must run in a cloud environment that is accredited to run Sensitive and Official Sensitive data, hosted within UK data centres and supported by security-cleared operations teams.

NEW GOVERNMENT CLOUD IS A GAMECHANGER

Recognising these obstacles to cloud adoption, Sungard Availability Services (Sungard AS) has launched its sovereign managed cloud platform, consulting and services for the UK public sector on Amazon Web Services (AWS).

With over 40 years of experience, the IT production and recovery provider have a solid track record of providing resilient, recoverable IT for more than 120

"SUNGARD AS' MANAGED CLOUD – AWS, UK SOVEREIGN SERVICE ENSURES DATA IS SECURE AND INCREASES THE RESILIENCE OF PHYSICAL AND DIGITAL INFRASTRUCTURE, ALL WHILE CUTTING COSTS."

Chris Huggett, Senior Vice President Sales, Europe and India

public sector organisations. The new Managed Cloud – AWS, UK Sovereign service has been specifically designed to enable the public sector to run Sensitive and Official Sensitive data on AWS, managed by a highly-skilled and security-cleared DevOps team provided by Sungard AS.

In order to achieve sovereign status, the service had to align with the National Cyber Security Centre (NCSC) Cloud Security Principles. These principles ensure that data is always located on UK soil and all personnel with access have the appropriate clearance including both SC+ (Security Cleared+) and NPPV (Non-Police Personnel Vetting), as well as being UK citizens.

The launch builds on Sungard AS' expertise with G-Cloud since 2014 with UK sovereign private cloud capabilities that currently underpin Official Sensitive workloads for critical national infrastructure, police forces and central government departments. This is in addition to the wide range of public sector private cloud implementations by Sungard AS that host publicly available, non-sensitive data.

"Sungard AS' Managed Cloud – AWS, UK Sovereign service further broadens our ability to help the public sector in managing risk and maintaining the sovereignty of their data," said Chris Huggett, Senior Vice President Sales, Europe and India at Sungard Availability Services. "Our relationship with AWS empowers UK public sector organisations to become more connected than ever before and manage risk effectively. It will ensure data is secure and increase the resilience of physical and digital infrastructure, all while cutting costs."

Sungard AS' services will help government bodies take new workloads and applications on to a public cloud platform that meets stringent sovereign service requirements. This will ensure that public sector workloads, with their specific needs for data sovereignty and privacy, can enjoy the innovation of AWS coupled with the resilience expertise of Sungard AS.

Sungard AS is something of an AWS expert, having achieved Managed Service Provider Partner status following a rigorous independent audit, and being a member of the AWS Solution Space Partner program having attained the AWS Storage Competency.

SUNGARD AS'S MANAGED CLOUD – AWS, UK SOVEREIGN SERVICE AT A GLANCE:

- A Managed Cloud – AWS service for workloads and data classified as 'Sensitive' and 'Official Sensitive'.
- The agility that the AWS platform provides, with the confidence that sensitive data is protected without having to build an AWS practice in-house.
- Hosting includes Critical National Infrastructure for services that are essential to maintain the security and wellbeing of the United Kingdom.
- SC+ cleared consulting services with a proven track record of providing sovereign services to both central and local government, including cloud, hosting and recovery for efficient adoption.
- SC+ cleared highly skilled DevOps team, providing 24x7 management of public sector AWS infrastructure.
- Cost savings resulting from replacing legacy IT infrastructure.

SIX STEPS TO A SUCCESSFUL MIGRATION

The process of migrating to the cloud can be complex but working with an experienced partner hugely increases the chances of a smooth transition.

Sungard AS works with your existing systems, whatever you may have, to develop a tailored environment that meets your needs quickly, flexibly and cost-effectively. It is one of the few cloud providers able to work with what is termed 'hybrid environments' – meaning IT that is both cloud-enabled and physical legacy systems. Whatever challenge you're facing, Sungard AS is likely to have worked with others who've been in a similar position and will apply what it had learned to help you.

Sungard AS' specialist cloud consultants follow a tried-and-tested process when helping organisations work through the obstacles to widen the number of applications and workloads that can be brought into the cloud:

1. MAP YOUR MOVE

Assess the needs and criticality of each application and workload, where they run and the business processes they support. Document the data protection, security and resiliency requirements of each, and their interdependencies, so you can take that into consideration as you plan your migration.

2. ALIGN APPLICATIONS AND INFRASTRUCTURES

One cloud does not fit all and hybrid cloud infrastructures are the norm today. Let the needs of each application and workload determine the cloud infrastructure it runs on, keeping data sensitivity, sovereignty and resilience needs in mind as you explore different clouds.

3. MAINTAIN DATA SOVEREIGNTY

To achieve sovereign status, the cloud services you use must align with the National Cyber Security Centre (NCSC) Cloud Security Principles.

4. USE AN AGILE TRANSFORMATION APPROACH

Sungard AS advises clients to get some quick wins by moving lower-risk workloads and applications first. Then, move on to those that are business-critical, with a higher impact if outages or security issues occur. Balance the need to accelerate cloud adoption with the need to minimise risks during the transition.

5. BUILD IN RESILIENCE AND RECOVERY FROM THE START

Use the requirements gathered about each workload and application to ensure the cloud environment they run on meets your specific resilience and recovery needs. This includes the Recovery Time Objective (RTO) – how quickly you want to recover – and Recovery Point Objective (RPO) – the maximum acceptable amount of data loss, measured in time – to prioritise their recovery, should disruption or disaster occur.

6. LOOK BEYOND TECHNOLOGY

Don't forget the process and people involved in widespread change. Clouds require you to orchestrate new ways of working, and across multi-cloud deployments. Take care to increase stakeholder awareness and alignment, documenting who is responsible for performing what operation and when. This can be critical to everyday resilience, as well as crisis management.

With only 3% of public sector organisations reporting they have completed their cloud journey, those wanting to enlist the help of a service provider at any point in the migration process will find Sungard AS a knowledgeable and reliable IT partner.

CASE STUDY

SUNGARD AS' PUBLIC SECTOR CLOUD EXPERTISE

THE CHALLENGE

A large central government agency needed a cloud partner it could depend on to host four important applications and provide a disaster recovery service to minimise downtime.

These applications are essential to help ensure the safety of UK citizens, prevent fraud, license the import and export of controlled drugs and precursor chemicals, and equip civil servants with the knowledge to do their jobs effectively.

THE SOLUTION

• **Government Cloud Services –** Sungard AS' fully-managed Government Cloud solution is aligned to the CESG Cloud Security Principles to host and process 'Official' data. Different levels of security are bridged via internet or Public Services Network (PSN)-connected services – essential for today's 'Digital by Default' citizen services to provide convenient access without compromising security.

• **Cloud-Based Recovery –** for the hardware and operating system by replicating data in real-time at one of Sungard AS' highly resilient data centres. The service provides continuous data protection by keeping a journal of data changes to enable restoration to a specific point in time in the event of a virus, hardware failure or software corruption.

RESULTS

- Supports the UK Government's 'Cloud First' policy.
- Speedy procurement process as G-Cloud suppliers have been pre-approved and Sungard AS maintains its services to the latest G-Cloud iteration.
- Two-year contract term provides flexibility to respond to technological advances.
- Standardised service specification enables the government department to compare 'like with like'.
- Ability to scale up quickly and easily according to demand for government services.
- Cost-savings are likely to be in line with 20% typical savings for G-Cloud contracts.

RESILIENCE LEADER

YOU are a champion of continuity. You think beyond backup to business resilience—ensuring critical data is always accessible. But when it comes to achieving resilience, changes to the production environment can be risky and complex.

CALL 0800 143 413
EMAIL government@sungardas.com

WE are Sungard Availability Services. We help transform IT and deliver resilient, recoverable production environments. As a recognised leader by multiple industry analysts for Disaster Recovery as a Service, we can calm the chaos of IT recovery. Imagine how we can help resilience leaders with everyday production systems.

Lead with resilience at www.sungardas.co.uk.

SUNGARD AVAILABILITY SERVICES®

Transforming IT for resilient business™