White Paper: **February 2023**

The State of UK Public Sector Cloud Management

Table of contents

Executive summary 3

Government initiatives driving cloud adoption 3

Key compliance considerations for the cloud 4

ENISA IAF (EU) 4

EU-U.S. Privacy Shield 5

EU Model Clauses 5

GDPR (EU) 5

Cyber Essentials Plus (UK) 5

PASF (UK) 6

Cloud management best practices 6

Migrate to the cloud 6

Build a cloud centre of excellence 7

Align business context to data 8

Optimise resource cost and utilisation 8

Centralise cloud governance 9

Integrate cloud and organisational KPIs 10

Conclusion 10

Executive summary

Over the past decade, public sector organisations in Europe, and specifically the United Kingdom, have been focused on digitally transforming government operations and services to improve quality, efficiency and effectiveness. Faced with government initiatives, policies for securing sensitive information, and restrictive budgets, government IT leaders are under immense pressure to adopt the public cloud.

Agencies and departments are now encountering new obstacles as they modernise legacy systems, seek to strengthen cybersecurity, and develop a cloud strategy. Effective cloud management does not begin or end with the development of a cloud strategy, however; government organisations need to execute on that strategy and maintain alignment with the organisation's mission over time. This will require collaboration and alignment between key stakeholders across finance, operations and security, commonly referred to as a cloud centre of excellence (CCoE).

In this white paper, you will:

- Learn about government initiatives driving cloud adoption
- Understand key compliance controls for evaluating cloud service providers
- Discover best practices for cloud management

Government initiatives driving cloud adoption

Throughout the past decade, public sector cloud adoption has increased as European countries focus on digitally transforming workflows, commonly referred to as e-government initiatives. The British exit from the European Union played a particularly critical role in the transformation seen across the UK as government agencies realigned resources and developed plans to adjust to this economic change.

To bolster their position in the digital economy, the UK documented its strategy related to digital transformation and the use of the public cloud. The UK Government Transformation Strategy 2017 to 2020 expanded upon the 2012 Government Digital Strategy by setting out to strengthen digital capabilities. More specifically, the UK government seeks to improve the experience for citizens, fully transform departments, improve collaboration across organisations, and ensure data is safeguarded.[1] Further, the UK government provides guidance, publications and declarations related to this strategy to aid public sector organisations as they adopt public cloud.

[1] GOV.UK. "Government Transformation Strategy 2017 to 2020."

Key considerations include:

- The Local Digital Declaration – This was established to develop common building blocks to help organisations build flexible services quickly and effectively. It invites all authorities and organisations to commit by signing.[2]
- The Technology Code of Practice – This is part of the Government Transformation Strategy and the Local Digital Declaration. It provides guidance to help organisations manage the full lifecycle of their technology. It also documents numerous standards across accessibility, APIs, security (from the National Cyber Security Centre), data protection, the Cloud First Policy, and more.[3]
- The Cloud First Policy – This was established in 2013 and mandates that the central government consider public cloud computing before hybrid cloud or private cloud options. This policy is also strongly encouraged to be followed by the rest of the public sector.[4]
- The Digital Marketplace – This is for public sector organisations to procure cloud software and services (the Government Cloud [G-Cloud] framework), digital outcomes and specialists, and data centre space.[5]

Key compliance considerations for the cloud

A broad set of compliance and regulatory controls have been put in place to standardise cloud use and safeguard personal and sensitive information. A few of the most notable regulations include the European Union Agency for Cybersecurity (ENISA) Information Assurance Framework (IAF), the EU-U.S. Privacy Shield, EU Model Clauses, the General Data Protection Regulation (GDPR), Cyber Essentials Plus, and the Police-Assured Secure Facility (PASF). These controls must be satisfied by government agencies as well as the cloud service providers they leverage.

ENISA IAF (EU)

ENISA contributes to EU cyber policy and helps Europe prepare for the cyber challenges of tomorrow. Within the ENISA Cloud Computing Risk Assessment is the IAF, which is a set of criteria designed to assess the risk of adopting cloud services, compare different cloud provider offerings, obtain assurance from the selected cloud providers, and reduce the assurance burden on cloud providers.[6]

[2] Local Digital Collaboration Unit. “Local Digital Declaration.”

[3] GOV.UK. “The technology code of practice.”

[4] GOV.UK. “Government Cloud First policy.”

[5] GOV.UK. “Buying and selling on the Digital Marketplace.”

[6] ENISA. “Cloud Computing Information Assurance Framework.”

EU-U.S. Privacy Shield

The EU-U.S. Privacy Shield Framework is a mechanism designed to provide the secure transfer of data between the European Union and the United States. Most businesses in the U.S. that trade in Europe will be required to join the EU-U.S. Privacy Shield Framework. The framework defines a set of requirements that govern the use and handling of personal data transferred from the EU, as well as access and dispute resolution mechanisms that participating companies must provide to EU citizens.

Companies must let individuals know how their data is processed, limit the purposes for which it is used, protect data for as long as it is held, and ensure accountability for data transferred to third parties.[7] In July 2020, the European Court of Justice challenged the EU-U.S. agreement and, as a result, affected companies now have to sign standard contractual clauses (non-negotiable legal contracts) drawn up by Europe.[8]

EU Model Clauses

The EU Model Clauses are standardised contractual clauses used in agreements between service providers and their customers to ensure any personal data leaving the European Economic Area (EEA) will be transferred in compliance with EU data protection laws and meet the requirements of the EU Data Protection Directive 95/46/EC.[9]

GDPR (EU)

The EU's GDPR protects data subjects' fundamental right to privacy and the protection of personal data.[10] With the introduction of GDPR, businesses operating in the EU have to implement a GDPR data retention policy. Any business that collects, processes or stores the personal information of an EU data subject must also implement a GDPR data retention policy.

Cyber Essentials Plus (UK)

Cyber Essentials is a UK government-backed scheme designed to help organisations assess and mitigate risks from common cybersecurity threats to their IT systems that could exploit customer data. Complying to this standard is a requirement for all UK government suppliers handling any personal data. Cyber Essentials Plus includes additional assurance by carrying out systems tests of implemented controls through an authorised third-party certifying body.[11]

[7] Microsoft. "EU-U.S. and Swiss-U.S. Privacy Shield Frameworks."

[8] BBC News. "EU-US Privacy Shield for data struck down by court." 16 July 2020.

[9] Microsoft. "European Union Model Clauses."

[10] Amazon Web Services. "General Data Protection Regulation (GDPR) Center."

[11] Microsoft. "UK Cyber Essentials Plus."

PASF (UK)

The National Policing Information Risk Management Policy sets the central standards and controls for law enforcement agencies assessing the risk of moving police information systems to the cloud. The policy requires that all national police services in the UK that store and process protectively marked or other sensitive law enforcement information must conduct a physical inspection of the data centre where their data will be stored. A successful assessment determines that a data centre qualifies as a PASF.[12]

Cloud management best practices

As government organisations transform their business, IT leaders will realise that legacy IT service management tools are not suitable for managing cloud applications and infrastructure. They will recognise the need for a solution that will streamline management, define governance policies, and help deliver on service levels. A cloud management platform can help government IT leaders track mission projects, ensure effective use of IT funds, and improve operational efficiency.

The following are six best practices for cloud management.

Migrate to the cloud

For governments just beginning their cloud journey, migration is a key component of their overall cloud strategy. There is tremendous pressure to accomplish a great deal with tight budgets and strict regulatory requirements. The first question to ask is which applications and workloads should be migrated to the cloud, taking into account whether they are critical in terms of operating costs or important for aligning to the agency's overall mission. Applications or workloads that do not fall into the aforementioned categories should be classified as a lower priority for migration.

Additionally, government agencies need to be aware of the resource impact of their applications as some applications may be more labour-intensive than others. Migrating to the cloud is a high-involvement process, and deciding which workloads to migrate is just the beginning. To comply with the Cloud First Policy, government agencies must carefully and thoroughly evaluate different cloud providers, such as Amazon Web Services, Microsoft Azure, and Google Cloud Platform, on their services offered and cost-effectiveness prior to considering hybrid cloud or private cloud alternatives. They will also have to choose a migration approach that best suits their organisation's needs. There are several options for migration, including lift and shift, partial refactor, full refactor, and incorporating software as a service or platform as a service.

[12] Microsoft. "UK Police-Assured Secure Facilities (PASF)."

Some cloud management platforms are able to help government agencies move faster in their migration process. For example, the Migration Assessment of VMware Tanzu CloudHealth® analyses your physical and virtual servers, and generates migration recommendations based on your existing configuration or utilisation for the cloud of your choice. Organisations can evaluate the cost of migrating to the cloud with a side-by-side comparison of on-premises costs compared against cloud configuration costs, and leverage recommendations based on asset types, region, reservations and projected costs—all of which can help ease the burden of migration planning.

Build a cloud centre of excellence

As the digitisation of public services continues, organisations are establishing a cross-functional group, commonly referred to as a CCoE, to support and govern the execution of the organisation's cloud strategy. Many organisations find that one of the most significant challenges is getting their staff and processes to adapt to a digital-first world. To overcome this, members of the CCoE are seen as advisors who provide best practices, architectural standards, and guidance to agencies and departments across three areas of excellence: cloud financial management, cloud operations, and cloud security and compliance. Members of the CCoE typically consist of stakeholders from each area of excellence along with various mission and business leaders. It's worth noting that although the term CCoE is broadly recognised, many organisations choose a name that is more closely aligned with the group's scope, such as cloud business office, cloud strategy office, or cloud community of practice.

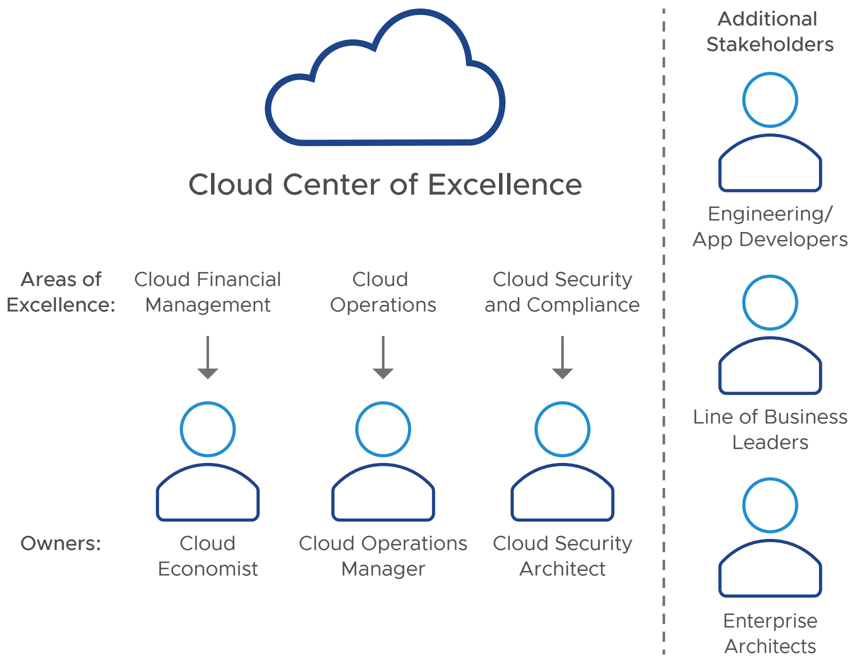

Figure 1: Sample structure of a CCoE.

Finding the right balance of guidelines and guardrails, and getting buy-in from lines of business and departments, can be challenging to navigate. The more a CCoE can build and nurture a community, the more successful it will be. Without a coordinated cloud strategy in place, measuring success across the organisation becomes more complex. A cloud management platform, such as Tanzu CloudHealth, can act as the hub of the CCoE. Tanzu CloudHealth helps organisations progress through four phases of cloud management maturity: visibility, optimisation, governance and automation, and business integration.

Align business context to data

As government agencies and departments increasingly consume cloud resources to modernise operations and deliver improved services to constituents, they need to maintain control over their cloud spend. A preliminary component to this budget adherence is ensuring visibility into cloud data. An initial but crucial task in the cloud is to develop a consistent tagging strategy to better identify and allocate spend and usage. Taking this a step further, many cloud management platforms have the ability to further group resources in a way that is meaningful to the organisation, such as building dynamic business groups by environment, department, owner or the like. In Tanzu CloudHealth, these are known as Perspectives.

With assets properly tagged and viewable, the CCoE can then drive accountability across the organisation and can show each group exactly how much they’re spending and what they’re spending it on. This will help the CCoE, and specifically the finance leader, establish an accurate budget. That way, when the next mandate to cut costs comes through, the team can make an educated decision on where to make adjustments. Additionally, the CCoE can use this granular visibility to ensure that everyone is working from the same data set, identify misconfigured and noncompliant assets, establish showback and/or chargeback, and determine key performance indicators (KPIs) and metrics to measure on an ongoing basis.

Optimise resource cost and utilisation

To eliminate waste and reduce operational costs in the cloud, government agencies need to continuously optimise their infrastructure. Optimisation can take several forms, such as decommissioning idle or unused infrastructure, rightsizing assets, and identifying opportunities to take advantage of pricing discounts offered by cloud service providers.

An easy way in which organisations save money is by finding and decommissioning actively running cloud resources no longer being used. Referred to as zombie infrastructure, these assets can include unused virtual machines, storage volumes no longer attached to a compute instance, old snapshots, and disassociated IP addresses, just to name a few.

In a growing cloud environment, organisations using manual analytic models across tens of thousands of resources often find it difficult and overwhelming to rightsize their environment—a challenge that worsens as they increase their use of cloud services or adopt a multi-cloud strategy. By analysing performance metrics (such as CPU, memory, network and disk) on a regular cadence, government IT teams can identify and make adjustments to these assets, and reclaim funds that can be reallocated to other mission-critical projects or initiatives.

Additionally, agencies can optimise costs by leveraging flexible pricing structures. For example, the leading cloud providers all offer some form of upfront monetary commitment to utilise specific asset types in return for a discount on compute costs. Known as Reservations, Savings Plans, and Committed Use Discounts, many organisations get caught up in the complexity of purchasing these discounts due to the number of options and the limited resources at their disposal for optimisation. A cloud management platform can be a trusted source to help with identifying purchase opportunities and managing these discounts throughout their lifecycle.

Centralise cloud governance

With restrictive budgets and lean hiring plans, it is critical for government agencies to maximise the resources at their disposal. Defining policies is the most efficient way to manage a scaling cloud infrastructure. Cloud governance policies can proactively alert on any irregularities, such as cost spikes, tagging compliance issues, security vulnerabilities, and more, across the different business units and departments that consume cloud resources. The CCoE often defines and enforces policies and governance throughout the agency.

Depending on the cloud management platform, the sophistication of policies can range from a simple email notification to an automated action, such as terminating unused infrastructure. Taking the initial step from governance alerting to governance automation can be daunting. It is advised to begin with automation within an approval workflow before action is taken and progress to full automation over time.

Tanzu CloudHealth provides the ability to add approvers or authorisers to governance policies for initiating change requests. Members of the CCoE team, for example, may be great candidates for authorisers within a cloud environment. Implementing cloud governance policies will free up staff for more mission-critical projects and can yield immediate cost savings.

Integrate cloud and organisational KPIs

The ultimate goal of cloud management is to fully integrate the cloud into your business, with the key being to embed cloud management processes into the day to day of users both inside and outside of IT. Organisations can begin by integrating with existing business systems, such as a governance risk and compliance solution or accounting software. It is important to note that integration goes beyond the technical components and extends to driving a cultural change across an organisation.

To measure the impact of cloud consumption, departments need to align cloud and operational KPIs with the organisation's business KPIs. These KPIs may include time to bring new services to market, compliance issues open, citizen satisfaction, and more.

At this phase, the CCoE should make it apparent how the cloud is:

- Reducing the dependency on legacy systems by minimising data centre footprint, hardware and operating costs
- Enabling new service delivery models and offering new digital experiences for employees and constituents
- Enhancing citizen engagement and satisfaction with government services
- Strengthening the organisation's security posture
- Contributing to the attraction and retainment of technology talent while improving the skillsets of the current workforce

Conclusion

The adoption of public cloud within the public sector continues to accelerate as more government agencies act on the mandates from European and UK initiatives. To successfully transition from legacy systems to the cloud, government agencies and departments need to establish a cloud centre of excellence to develop and execute on their digital transformation strategy.

Government agencies do not need to be hesitant to migrate to the cloud due to compliance controls or limited in-house cloud expertise. Tanzu CloudHealth helps government organisations deliver new and improved services to their constituents by accelerating migration to the cloud, ensuring effective use of IT funds, and improving operational efficiency.