Cloud Services and the Government Security Classifications Policy

ukcloud | white paper

Pure Commitment.
T 01252 303 300
ukcloud.com

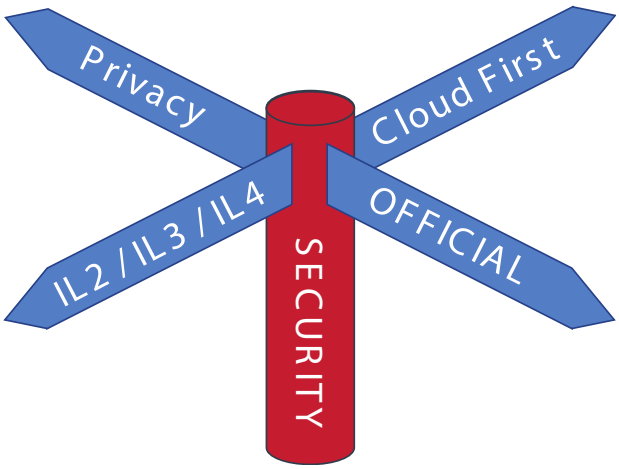
Executive summary

The UK government has increasingly been encouraging the use of cloud services instead of traditional IT solutions as it seeks to create more cost-effective and agile platforms as part of the Government ICT Strategy. To support this strategy the government has implemented a number of policies and initiatives to make the adoption and use of cloud services easier.

One example is the Cloud First policy, an initiative designed to ensure that central government organisations have a strategy to consume cloud services and deter them from continuing to perpetuate non-cloud solutions. Another example is the G-Cloud framework, established by the government to make it much easier for SME providers to create and sell cloud services, and for public sector organisations to buy them.

The government continues to remove potential barriers to cloud services and enable public sector organisations to evaluate, procure and consume them. The Government Security Classifications Policy (GSCP) replaced the previous Government Protective Marking Scheme (GPMS) in 2014 after a period of parallel running.

The GSCP replaces the previous six Impact Levels (ILs) with just three classifications: OFFICIAL, SECRET and TOP-SECRET. Public sector organisations are encouraged to make their own decisions about which controls are required to appropriately protect their data and systems. In essence, the new GSCP aims to remove the "CESG says no" misconception that was constraining the adoption of and transition to agile cloud services.



A potential problem is that, although public sector organisations are now clearly encouraged by the GSCP to make their own decisions, rather than be guided by CESG (the independent Technical Authority within government), issues and concerns remain. These include:

- Privacy concerns (eg US National Security Agency surveillance)
- Sovereignty issues (eg US Stored Communications Act)
- Integrity issues (eg the OpenSSL Heartbleed bug)

All of these may make organisations less confident about embracing cloud-based services.

In addition, some Senior Information Risk Officers (SIROs) are struggling to understand how assets previously classified at IL3 or IL4, which may now be classified as OFFICIAL, can be securely deployed on cloud platforms that might only have been suitable for assets classified as IL2 in the past.

This white paper provides public sector organisations with advice and guidance to help them make appropriate use of cloud services without compromising the confidentiality, integrity or availability of the information which makes up their digital and shared services. Because not all cloud services are created equal, this paper explains how public sector organisations can safely select appropriate cloud services, even for the most precious of data assets (eg information that was previously classified at IL4).

In this white paper

Introduction to cloud security **4**

The Government Security Classifications policy **5**

Government guidance for security and the cloud **6**

Transitioning to the new security classifications **10**

Not all clouds are created equal **12**

The role of partners **17**

Summary **18**

About UKCloud **19**

Introduction to cloud security

Cloud services can help deliver more dynamic and agile ICT solutions in terms of service demand and resource availability. They also offer improved availability and significant cost savings. The G-Cloud Framework and Digital Marketplace make it easier for the UK public sector to assess a wide range of services available from an extensive list of suppliers. They also provide a quick, compliant and transparent way to award contracts and place orders.

Services offered through the GCloud Framework are described in accordance with the Government Security Classifications Policy (GSCP) — they must be aligned to OFFICIAL rather than to Impact Levels 2 and 3 (IL2 and IL3) as was previously the case.

Cloud services offered through previous GCloud Framework iterations could be pre-accredited by the CESG Pan Government Accreditor (PGA), but since G-Cloud 6 that's no longer the case. Instead, cloud service providers must be more transparent about the security features of their cloud services, in line with the CESG Cloud Security Principles.

The goal is for cloud service providers to differentiate their services based on the depth of assurance each service offers the consuming organisation. The premise is that organisations will determine for themselves how much assurance they require to suit their individual workloads and risk appetite.

To demonstrate assurance, a cloud service provider must:

- Describe the security characteristics of cloud service
- Provide suitable evidence that those characteristics are robustly implemented

The Digital Marketplace facilitates the former as it requires the security characteristics of G-Cloud services to be described in line with the published CESG Cloud Security Principles. This enables public sector buyers to shortlist potential cloud services based on their advertised security characteristics.

Buyers should then expect a further layer of detail from suppliers about how the cloud service implements each of the CESG Cloud Security Principles.

Finally, buyers should request evidence from the cloud security provider that each of the security characteristics is robustly implemented. Clearly, they should favour evidence of independent validation rather simply rely on self-affirmation from the cloud service provider.

Based on this information, public sector organisations can make informed risk-based decisions about which cloud services best meet their specific security requirements.

The Government Security Classifications policy

The Government Security Classifications Policy (GSCP) introduced a three-tier classification system which doesn't directly map onto the six Impact Levels within the former Government Protective Marking Scheme (GPMS).

The previous SECRET and TOP SECRET classifications (formerly IL5 and IL6 respectively) stay the same. However, the other categories (IL0 to IL4) have been brought together into a single OFFICIAL classification (see Figure 1).

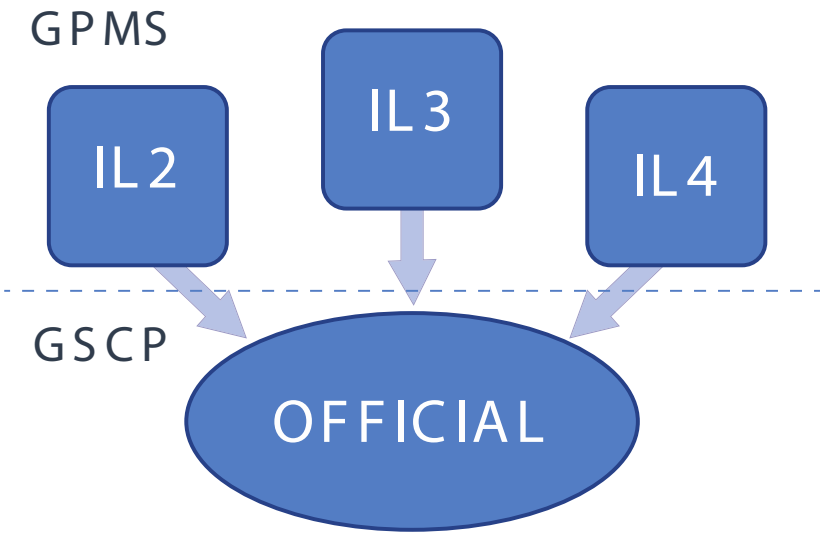
A sub-category of OFFICIAL-SENSITIVE has been introduced to enhance certain management and handling controls for OFFICIAL data deemed to be especially sensitive. But OFFICIAL SENSITIVE doesn't specify additional mandatory technical controls, as it's intended that this data be hosted on the same platforms as OFFICIAL data.

The GSCP fundamentally clarifies the responsibility for risk and the decisions that an organisation takes as to how risks are managed. Each public sector organisation is empowered to:

- Properly assess its potential cloud service providers
- Satisfy itself that risks to its information are properly managed and controlled at every stage of the supplier engagement

Making an informed decision is vital to ensuring the protection of a public sector organisation's data, so the government has published a range of resources to help guide and inform that decision-making process. They're described in the next section.

Figure 1. Mapping GPMS IL2–IL4 to GSCP OFFICIAL classification



Government guidance for security and the cloud

Under the GPMS, CESG (the independent Technical Authority within government) provided guidance — including Good Practice Guides and Architectural Patterns — and formal accreditation services — such as Pan Government Accreditation (PGA) — to ensure a consistent level of security across the public sector for each Impact Level.

Under the GSCP, each public sector organisation must determine the security characteristics it requires for appropriate protection of its data and systems. However, some public sector organisations acknowledge that they aren't information security specialists, and others simply don't know where to start. To help, the Cabinet Office, CESG and Government Digital Services (GDS) have published specific guidance, outlined below.

Cloud Security Principles

CESG has published a set of guidance centred on 14 Cloud Security Principles[1] that public sector organisations should consider when evaluating a cloud service. These principles cover a range of people, process and technology controls, for example:

- The location and physical security of the data centres which host the cloud service
- The information security governance procedures implemented by the cloud service provider (CSP)
- The suitability of the CSP's staff as determined by appropriate personnel clearance and/or vetting

It is for the consumer of the service to decide which of the security principles are important to them in the context of how they expect to use the service.

Based on the 14 Cloud Security Principles, most public sector organisations will prefer cloud services delivered by service providers who meet the following criteria:

- Can demonstrate robust independent assurance (eg experience as a PGA-accredited or PSN-accredited supplier)
- Are UK sovereign, with UK data centre facilities and SC cleared personnel
- Offer commercial agility, competitive pricing and clarity in engagements
- Understand UK data protection legislation and reduce risks relative to foreign deployments
- Can provide differentiated platforms — for example, a lower-security platform with broad internet connectivity, and a higher-security platform exclusively connected to Government Secure Networks such as PSN and N3

1 https://www.gov.uk/government/publications/cloud-service-security-principles

Government Service Design Manual

The GDS was created to deliver transformational digital projects across government (starting with GOV.UK), and to pioneer the introduction of new skills and approaches to government, such as agile software development. The Government Service Design Manual[2] has become the standard used across government in the delivery of digital projects, as it has captured much of the good practice that helped to deliver GOV.UK and many other digital exemplars.

The Service Design Manual offers specific guidance around the approach to security. It promotes the idea of security as an enabler rather than a constraining factor ("security says no"). GDS suggests that "security must be proportionate", which supports the idea of CSPs having differentiated platforms exposed to different risks.

Protecting information from valid threats to its confidentiality, integrity and availability is an enabler of digital services. Without such protection, digital services would be impossible or unsafe.

For example, if a digital service is citizen facing, a cloud service exposed to the internet is a proportionate risk. For shared services within government which are internal facing, a PSN-connected cloud service may be preferable because exposure to the internet could be a disproportionate and unnecessary risk.

The Service Design Manual also urges consuming organisations to 'evaluate the privacy risks'. There are many examples of security breaches that have compromised information confidentiality and threatened the privacy of citizens. Public sector organisations should prefer cloud services delivered and operated entirely within the UK, hosted in secure UK data centres and managed by UK based staff who have been subject to formal SC clearance.

By using a UK sovereign service, organisations can be confident they comply with UK laws (eg the UK Data Protection Act), and that privacy isn't threatened by foreign legislation (eg the US Patriot Act) or other activities by foreign actors (eg US National Security Agency surveillance).

G-Cloud and the Government Security Classifications

GCloud 6 introduces better alignment of cloud services with the CESG Cloud Security Principles. This enables suppliers to differentiate their cloud services based on the degree to which:

- Each Principle has been implemented
- The implementation has been independently validated

Customers can therefore shortlist cloud services based on their security characteristics, and evaluate the robustness of the claimed level of assurance by reviewing evidence of independent testing and validation offered by the cloud service provider.

2 https://www.gov.uk/service-manual

Suppliers will complete a number of pre-defined security statements asserting how their services meet the Cloud Security Principles.

For more guidance on the extent to which cloud services are suitable for different types of OFFICIAL data, see the section "Not all clouds are created equal" on page 12

Cyber Essentials Scheme

A primary objective of the UK government's National Cyber Security Strategy is to make the UK a safer place to conduct business online. In line with this objective, the Department for Business, Innovation & Skills (BIS) launched the Cyber Essentials Scheme[3]. It's designed to help organisations ensure they mitigate the risk from most common internet-based threats that use "commodity" capabilities.

Unlike the other government guidance referenced above, the Cyber Essentials Scheme is targeted at smaller enterprises delivering products and services to the UK public sector, rather than larger organisations. It's also aimed at their internal IT systems rather than at platforms used to underpin the provision of a cloud service to customers.

The Cyber Essentials Scheme provides a foundation level of guidance to ensure the most common internet risks are mitigated. Other guidance, such as the CESG Cloud Security Principles (especially the Consumer guide which describes principle 14 in detail), build on and extend the guidance provided by the Cyber Essentials Scheme.

There are two levels of Cyber Essentials certification:

- Cyber Essentials certification is awarded on the basis of a verified self-assessment which is then verified by an independent certification body to assess whether an appropriate standard has been achieved. This level offers a basic level of assurance.
- Cyber Essentials Plus offers a higher level of assurance through the external testing of the organisation's cyber security approach.

To demonstrate the breadth and depth of security that has been implemented across their organisations, CSPs should achieve independent certification at the Cyber Essentials Plus level.

To achieve certification, IT systems should be aligned with the requirements of the Cyber Essentials Scheme and service providers should enable the five basic controls required by the Scheme (listed below).

These control areas are already covered in existing frameworks such as the ISO 27001 standard, but the selection of these topics by the Scheme reflects their importance in preventing unauthorised access and malicious activities by internal and external threat actors.

1. **Boundary firewalls and internet gateways.** The service should be protected by both perimeter firewalls and a layer of virtual firewalls which are entirely self-managed. The platform may also need to be further protected, possibly by a cross domain solution, which further controls the level of internet access into the environment.
2. **Secure configuration.** The service should be secure by default. A customer's self-managed firewall should be pre-configured to block all access until they specify traffic they explicitly want to allow to pass. The supplier should also provide a number of operating system images in its service catalogue which have also been designed to be secure by default.

3 https://www.cyberstreetwise.com/cyberessentials/files/scheme-summary.pdf

3. **User access control.** The management portal should provide full role-based access control (RBAC) to enable customers to control which of their users can access their environment.
4. **Malware protection.** The platform should be fully protected against malware. Customers should be able to select and implement their own malware protection within their virtual data centre, by having full root/administrative control over the servers and operating systems hosted on the cloud platform.
5. **Patch management.** The platform should be regularly patched with security and infrastructure updates, and customers should be able to fully control the patch management regime that applies to their solution. Customers should have full root/administrative control giving them full permissions to apply patches. The supplier should also make certain patch repositories available within a higher-security domain to further help with patch deployment.

CERT-UK

CERT-UK[4], the UK Computer Emergency Response Team, works closely with industry, government and academia to enhance the UK's level of cyber resilience. Like the Cyber Essentials Scheme, CERTUK is part of the National Cyber Security Strategy.

It is responsible for:

- Managing national cyber security incidents
- Providing support to critical national infrastructure companies to handle cyber security incidents
- Promoting cyber security situational awareness across industry, academia and the public sector
- Being the single international point of contact for co-ordination and collaboration with other national CERTs

CERT-UK partners with organisations such as GovCERT, the UK Government's Computer Emergency Response Team. Some responsible CSPs have already implemented protocols to work with GovCERT. These same protocols can be extended to support initiatives such as sector-based WARPs (Warning and Advisory Reporting Points), and can facilitate membership of the CERT-UK Cyber Information Sharing Partnership (CISP).

Although CERT-UK focuses on management of cyber security incidents, it also aggregates best practice advisories such as the "10 Steps to Cyber Security"[5] published by BIS and the "20 Critical Controls"[6] published by the Centre for the Protection of National Infrastructure (CPNI).

4 https://www.gov.uk/government/news/uk-launches-first-national-cert

5 https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility

6 http://www.cpni.gov.uk/advice/cyber/Critical-controls/

Transitioning to the GSCP security classifications

CESG has published guidance on how to use the Cloud Security Principles when making risk-management decisions[7]. Consistent with CESG's guidance, Cabinet Office also recommends that public sector organisations continue to adopt good Risk Assessment and Risk Management processes (eg IS1/IS2) to evaluate the risks to information assets. Under IS1/IS2, it remains appropriate to reference the Business Impact Level tables. Organisations that have already determined the business impact of a loss of confidentiality, integrity or availability (denoted as IL2, IL3 or IL4) may find this section useful in considering what to look for under the OFFICIAL classification of the GSCP.

Transitioning from IL2 to OFFICIAL

It should be relatively simple to transition IL2 assets to the GSCP OFFICIAL classification. Under the GPMS, cloud services suitable for IL2 had to follow commercial best practice as evidenced by an appropriately scoped ISO 27001 certification from a UKAS-recognised audit body. Under the GSCP, the OFFICIAL tier has a similar requirement.

Consumers should seek assurance that CSPs have actually implemented and operate commercial good practice controls. The GCloud PGA by CESG is a useful benchmark — many cloud services have previously achieved formal CESG PGA accreditation at IL2. Cloud services which haven't achieved this relatively low bar or which aren't PSN accredited should be thoroughly scrutinised.

Consumers should also consider the legal jurisdiction of any cloud service they're evaluating. Many cloud services operate outside UK jurisdiction in territories such as North America and mainland European Union, which may pose an additional risk to the confidentiality (eg privacy) and availability of the service being consumed. An example is the ongoing case in which a US court has ordered Microsoft to release data, even though it was held in Ireland[8].

Transitioning from IL3 to OFFICIAL

IL3 assets have a more difficult transition to the OFFICIAL classification. Under the GPMS, cloud services suitable for IL3 were expected to adhere to CESG Good Practice (such as limiting connectivity to a trusted community of users, eg GSI). The suitability of cloud services for IL3 was previously evidenced by CESG PGA and PSN accreditation, both of which involved extensive documentation, auditing and technical testing by independent security specialists.

Under the GSCP, the OFFICIAL tier doesn't enforce these requirements. Consumers should therefore seek evidence that CSPs have actually implemented and operate appropriate CESG Good Practice controls (such as protective monitoring that complies with Good Practice Guideline 13), as these controls are still relevant regardless of the switch to the GSCP. It's essential that the CSP can provide evidence of independent testing and validation, such as PSN Accreditation for the Protected service.

7 https://www.gov.uk/government/publications/cloud-security-guidance-risk-management

8 http://www.bbc.co.uk/news/technology-27191500

Comparatively few cloud services were able to achieve the previous CESG PGA at IL3, or currently hold PSN Accreditation for the PSN Protected service, which may make it tempting for customers to consider using non-accredited or self-accredited cloud services.

Public sector organisations need to carefully evaluate the risks of doing this. They should consider the legal jurisdiction of any cloud service they're evaluating (as mentioned above). Many cloud services operate outside UK jurisdiction which may pose an additional risk to the confidentiality (eg privacy) and availability of sensitive assets. For assets previously classified at IL3 or above, and now classified as OFFICIAL, it's essential that cloud providers host and manage their cloud service within the UK.

Finally, a subset of assets previously at IL3 (eg a register of vulnerable adults) could be considered for managing using the OFFICIAL SENSITIVE sub-category. Information in this sub-category should be more tightly controlled and available on a strict "need to know" basis. One way to achieve this is to host them on a cloud platform that's connected only to the closed community of PSN users, rather than openly connected to the internet. This is often called a community cloud (rather than a public cloud).

Some CSPs offer both types of cloud service; some exposed to the internet and other directly connected only to Government Secure Networks (such as PSN and N3). For services connected to the PSN, consuming organisations should look for the enhanced assurance provided by independent PSN accreditation for the PSN Protected service.

Transitioning from IL4 to OFFICIAL

Legacy IL4 assets have the most difficult transition to the GSCP OFFICIAL classification. Under the GPMS, cloud services suitable for IL4 were expected to adhere to even stricter controls related to people, processes and technology than those suitable for IL3.

Given the potential impact of failing to maintain the confidentiality, integrity or availability of such assets, consuming organisations must look for the following over and above the relatively low baseline controls allowed by the OFFICIAL tier:

- UK jurisdiction. Data assets must stay in the UK, hosted in secure UK data centres operated by UK-based security-cleared staff. The risk of such sensitive data being subject to foreign legislation (eg the US Patriot Act) or foreign surveillance is intolerable for most risk owners.
- Community cloud. Data assets at IL4 must be tightly controlled and shared only across Government Secure Networks such as PSN and N3. Hosting such assets on a public cloud which is openly exposed to the internet is likely to be considered a disproportionate risk. Some CSPs can facilitate indirect access between comparatively secure cloud platforms and internet-facing cloud platforms, to support initiatives such as secure citizen access.

Not all clouds are created equal

With the adoption of the GSCP, public sector organisations are empowered to accelerate their consumption of cloud services by silencing the "CESG says no" mentality that could be an unfortunate aspect of the previous GPMS.

However, public sector organisations must take care that they don't simply move from one extreme (security as a blocker) to the other by assuming — incorrectly — that all cloud services are created equal.

> **The new Security Approach is a more transparent way for suppliers to assert how they are securing their services, and the methods of supporting assurance they are using. There is no wrong answer. This approach is designed to enable buyers to select services with an informed view as to the status of the security of that service.**
>
> **— Digital Marketplace blog**

As CESG acknowledges, many cloud services will meet only a subset of the core Security Principles, and an even greater number of cloud services will provide only the light assurance of self-affirmation, with no independent validation or measurement of how well — or how poorly — the Security Principles are being implemented and operated.

In the document 'FAQ Sheet 2: Managing Information Risk at OFFICIAL'[9], Cabinet Office identifies three categories of cloud services:

- **Accredited public cloud services.** Cloud services which previously achieved CESG PGA IL3 or currently hold PSN Accreditation for the encrypted overlay (Protected service).
- **Assured public cloud services.** Cloud services which previously achieved CESG PGA IL2 and can demonstrate independent validation of security assertions.
- **Unassured cloud services.** Cloud services which have never achieved CESG PGA and rely mainly on self-affirmation. These include global cloud services such as Amazon Web Services (AWS) and Dropbox.

Based on the Cabinet Office guidance, it's clear that those three categories of cloud services meet the requirements of systems classified as OFFICIAL to varying degrees:

- Only **accredited cloud services** (as evidenced by PSN Accreditation) are suitable for all OFFICIAL information
- **Assured cloud services** (as evidenced by independent validation) are expected to be suitable for most OFFICIAL information.
- **Unassured cloud services** are said to be suitable for **some** OFFICIAL information only

9 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/286667/FAQ2_-_Managing_Information_Risk_at_OFFICIAL_v2_-_March_2014.pdf

The value of independent validation for Assured OFFICIAL

UKCloud has built a unique cloud services platform: entirely UK sovereign, housed in two geographically separate UK data centres operated by UK-based security-cleared staff.

UKCloud has always held information security and transparency as core values. It has received independent certification from LRQA against international standards for information security (ISO 27001), IT service management (ISO 20000) and quality management (ISO 9001).

In addition, UKCloud was one of the first providers to achieve CESG PGA at IL2 and PSN Accreditation, which independently validates the effectiveness of the systems and controls UKCloud has implemented.

The platform is provided exclusively to UK public sector organisations. All our cloud services are provided on a true utility model: no-upfront costs, no extended lead time, and no minimum contract term — just genuine usage-based billing (per virtual machine per hour, or per GB per month).

There is an alternative to the global clouds run by AWS, Google and Microsoft. Beware of unsubstantiated supplier assertions; always seek independent, traceable verification that cloud services offer security controls which are appropriate for their data.

The value of PSN Accreditation for Elevated OFFICIAL

In addition to its Assured OFFICIAL platform, UKCloud operates a second platform — UKCloud Elevated OFFICIAL.

Whereas the Assured OFFICIAL cloud platform is directly connected to the internet, the Elevated OFFICIAL cloud is connected exclusively to Government Secure Networks such as PSN and N3.

The Elevated OFFICIAL platform enables the provision of true cloud services within a secure, closed community of like-minded users. It can be considered a safe environment for solutions such as shared services containing sensitive information assets that must never be vulnerable to untrusted internet traffic or unknown organisations.

Consumers can take additional assurance from the previous CESG PGA at IL3 and current PSN Accreditation that our cloud services hold for the PSN Protected service (encrypted overlay). UKCloud is still one a very small number of organisations providing compute, storage and collaboration cloud services which have been both Pan Government Accredited and PSN Accredited.

Comparing cloud platforms using Cloud Security Principles

Under the GSCP, consuming organisations can select general public cloud platforms if they consider the security offered to be appropriate for their data. The table shows how the our cloud platforms compare with a typical public cloud platform.

Cloud Security Principle	Typical public cloud	UKCloud Assured OFFICIAL cloud	UKCloud Elevated OFFICIAL cloud
NIST cloud model	**Public cloud**	**UK-sovereign public cloud (designed for UK public sector)**	**UK-sovereign public cloud (designed for UK public sector)**
Security and assurance			
Data centre locations	Varies — typically North America or continental Europe	Both data centres in the UK, separated by more than 100km	
Location of service management	Varies — typically North America, continental Europe or continental Asia	Entirely within the UK from two secure sites, both Pan Government Accredited to IL3	
Security of data centre	Varies	Both data centres assessed by CESG Pan Government Accreditors as part of UKCloud's PSN Accreditation, and independently capable of achieving SECRET status. Approved by the Home Office for police "blue light" data.	
Vetting of staff	Varies	All employees are subject to security clearance. All operational staff with access to the UKCloud platform undergo a formal Security Check (SC) and Non-Police Personnel Vetting (NPPV). All employees have signed the Official Secrets Act and benefit from regular Information security education.	
Protective monitoring	No	UKCloud has implemented a Protective Monitoring service across all cloud service platforms. Protective Monitoring is implemented in alignment with CESG Good Practice Guide, number 13 (GPG13) and provides a robust and effective audit and monitoring solution. Protective Monitoring is operated on a 24/7 basis by trained Security Analysts.	

Cloud Security principle	Typical public cloud	UKCloud Assured OFFICIAL cloud	UKCloud Elevated OFFICIAL cloud
Security and assurance (cont.)			
CESG Pan Govt. Accredited (IL2)	No	G-Cloud 1 through G-Cloud 5	N/A
CESG Pan Govt. Accredited (IL3)	No	N/A	G-Cloud 1 through G-Cloud 5
PSN Accredited	No	Yes — PSN Assured	Yes — PSN Protected
Suitable UKAS ISO 27001, ISO 20000 and ISO 9001 certifications	Not usually	Yes (LRQA)	Yes (LRQA)
Cyber Essentials Plus Scheme	No	Yes	Yes
Connectivity options			
Direct resilient internet connectivity	Yes	Yes	No (indirect/controlled via Cross Domain Guard)
1Tb+ DDoS mitigation service	No	Yes	n/a
CPA Foundation Grade VPN support	No	Yes	Yes — including a secure remote access service
PSN connectivity	No	PSN Assured	PSN Protected
RLI connectivity	No	No	Yes
JANET connectivity	No	Yes	No
N3 connectivity	No	Yes	Yes (with appropriate technical controls)
Private circuit support	No	Yes (CAS-T)	Yes — CAS(T) with additional encryption

The table shows that typical public cloud platforms can't provide the breadth or depth of security that UKCloud provides as standard. UKCloud's services have been independently and repeatedly inspected under CESG GCloud Pan Government Accreditation, PSN Accreditation and certification under commercial schemes such as ISO 27001. UKCloud is one of the very first organisations to have successfully achieved both Cyber Essentials and Cyber Essentials Plus certification. All UKCloud services are available on the same commercial terms as many generic public cloud services — yet, as the table shows, the UKCloud platforms address a much wider range of UK public sector–specific challenges.

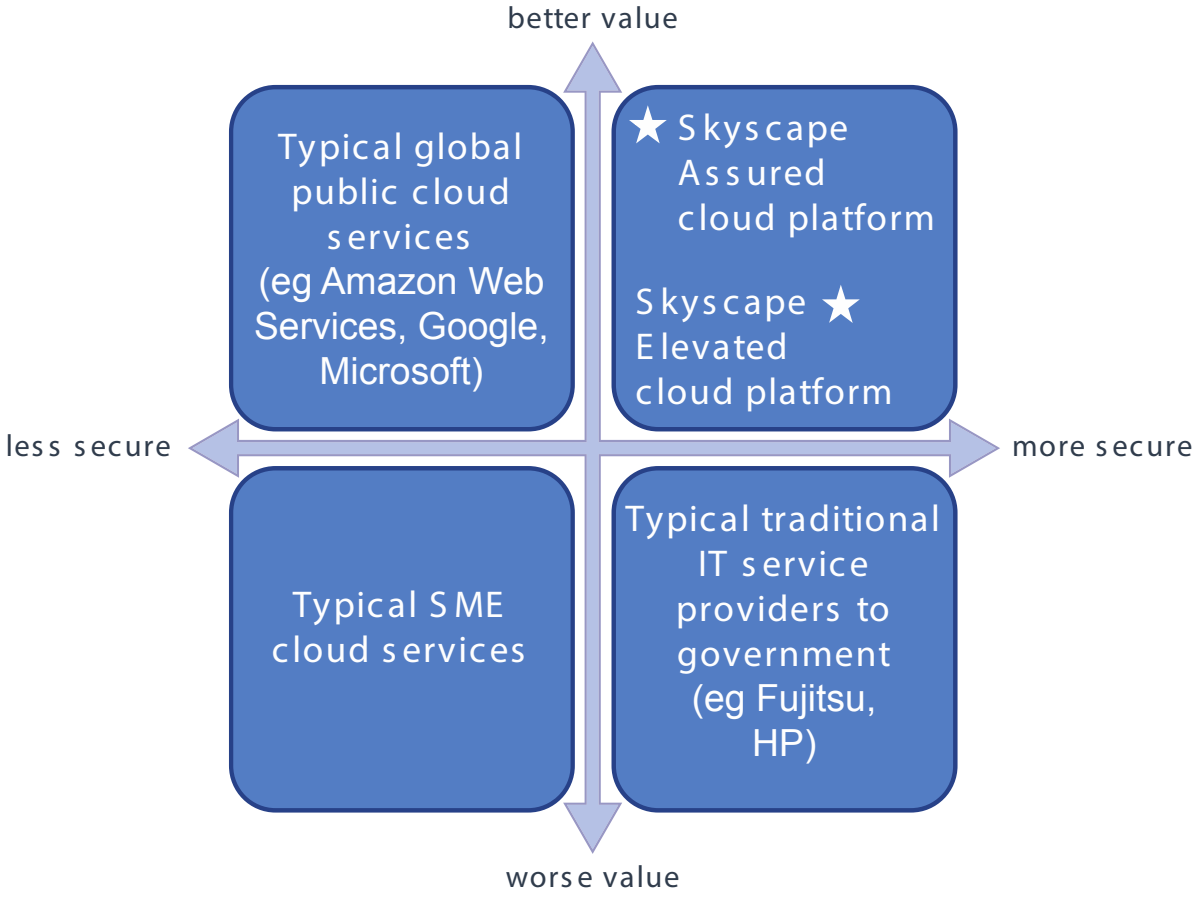
Figure 2 shows the relative positioning of CSPs when considering appropriate security (x-axis) and value (y-axis).

Providers who score well against the security axis (typically long-term suppliers to government) often don't provide best value as they typically require upfront investment, minimum contract terms, monthly billing (regardless of usage) and so on.

Public cloud providers who score well against the value axis often don't provide security that's appropriate for UK public sector organisations (for example, there is misalignment with Cloud Security Principles in areas such as offshore data centres, offshore service centres, or unvetted staff).

UKCloud uniquely combines the highest levels of independently assured security with the highest levels of value through true utility billing and flexible commercial models.

Figure 2. Relative positioning of cloud service providers: value vs security



The role of partners

UKCloud has introduced 'Optimised for OFFICIAL', a product mark designed to give UK public sector organisations assurance that the cloud services bearing this mark are closely aligned to CESG Cloud Security Principles.

Figure 3. The UKCloud 'Optimised for OFFICIAL' product mark

Each of our cloud services will bear this mark along with selected products and services from over 200 of our partners. Our partners provide value-added cloud services ranging from Software as a Service (SaaS) offerings (powered by UKCloud) to specialist cloud services such as management, transition and transformation services.

Summary

Based on the government guidance described in this document, UKCloud suggests the following top tips for navigating GSCP for your Digital by Default and Cloud First strategy.

☑ **UK jurisdiction**. Data assets should remain physically within the UK, hosted in secure UK data centres and operated by a UK company. UKCloud believes the risk of sensitive data being subject to foreign legislation (eg the US Patriot Act) or foreign surveillance is a significant issue for many risk owners, and a valid concern to data subjects.

☑ **Vetted staff**. All employees and contractors with access to the cloud services platforms should be subject to extensive vetting such as government Security Check (SC) and non-Police Personnel Vetting (NPPV). All employees and contractors should also undergo formal and regular information security training and should have signed the Official Secrets Act.

☑ **Broad connectivity.** The cloud services platform should be resiliently connected to the internet as well as to Government Secure Networks such as PSN, N3 and legacy networks like GSI. The cloud service should be formally PSN accredited to show it's a recognised PSN-compliant service.

☑ **GPG13 Protective Monitoring**. The cloud service should benefit from robust Protective Monitoring, implemented in accordance with CESG Good Practice Guide number 13 (GPG13), and should be independently assured to provide a robust activity auditing and monitoring solution.

☑ **Multiple cloud platforms**. One size doesn't fit all — a cloud platform exposed to wider internet threats serves different public-sector use cases to a cloud platform that's safely and exclusively connected to Government Secure Networks (eg a community cloud).

☑ **Cross Domain Solution**. Given that some OFFICIAL systems are less secure than others, public sector organisations should require a Cross Domain Solution which supports CESG-recognised scenarios to facilitate controlled citizen access to sensitive data sets.

☑ **Independent validation**. Don't trust self-accreditation — look for cloud services that have been independently validated and tested by recognised authorities (such as CESG). Be sure to review and evaluate the service provider's evidence that the implementation is robust.

☑ **Cloud Security Principles**. Look for cloud services which have implemented all 14 CESG Cloud Security Principles. Ask for documentation aligned to the CESG Cloud Security Principles to make it easy for you to evaluate your risks.

About UKCloud

UKCloud provides a true public cloud for the exclusive use of UK Public Sector organisations. We are dedicated to helping our customers gain value from the agility and cost savings of using a sovereign, assured cloud platform.

Focusing solely on Public Sector customers, we are able to provide a leading cloud proposition that delivers outstanding value and capability. This ultimately benefits the UK taxpayer, citizens and businesses by enabling Public Sector organisations to deliver better services through technology.

Here's how:

- **We're focused on cloud.** Delivering a true cloud platform that is massively scalable, flexible, assured and cost-effective – and customers only pay for what they use.
- **We're open. You are never locked in**. Using industry standards and open source software our platform gives customers the flexibility and choice to transition and transform their applications and deploy across multiple cloud solutions.
- **Dedicated to the UK Public Sector.** Our business is designed specifically to serve and understand the needs of public sector organisations, and is UK sovereign, with UK cleared staff and we pay UK taxes.
- **We develop communities.** We bring together communities of users that are able to share datasets, reuse code, test ideas and solve problems that enhance services and benefit the UK citizen.
- **Customer engagement.** We will only be successful if our customers are successful. We embody this in the promise: Easy to adopt. Easy to use. Easy to leave.

Supporting both cloud native and enterprise applications — based on VMware, OpenStack and Oracle stacks — the platform is used extensively to host both citizen web applications, and internal facing applications only available through secure government networks.

Our industry-leading platform is built on the unique and cutting-edge technologies of the UKCloud Cloud Alliance — QinetiQ, VMware, Cisco, EMC and Ark Data Centres — which continually drives innovation and product development, at the lowest price to meet the needs of the UK Public Sector.

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

UKCloud. The power behind public sector technology.

More information

For more information about UKCloud and how we can help you, please send an email to info@ukcloud.com

UKCloud Ltd
A8, Cody Technology Park
Ively Road, Farnborough
Hampshire, GU14 0LX

T 01252 303 300
E info@ukcloud.com
ukcloud.com
@ukcloudltd

UKC-GEN-127-D • 08.2016