CLOUD SERVICES AND THE GOVERNMENT SECURITY CLASSIFICATIONS POLICY
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 significant 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 fact that through the G-Cloud framework the government has made it much easier for SME providers to create and sell cloud services whilst also making it much easier for all public sector organisations to procure those services.

However, it has been observed that some UK public sector organisations have misinterpreted CESG guidance around Impact Levels under the Government Protective Marking Scheme (GPMS) creating an unnecessary barrier to consume cloud services. This has continued to happen despite some cloud services having achieved CESG Pan Government Accreditation and/or PSN Accreditation at IL3.

On 2 April 2014, the Government Security Classification Policy (GSCP) was introduced which will ultimately replace the previous GPMS after a period of parallel running. The GSCP replaces the previous six Impact Levels (ILs) with just three classifications; OFFICIAL, SECRET and TOP-SECRET.

As there is no mapping between the previous Impact Levels and the new categories, public sector organisations are encouraged to make their own decision as to what controls are required for the appropriate protection of their data and systems. In essence, the new GSCP aims to remove the ‘CESG says no’ misconception that is restraining the transition to agile cloud services.

Similar to the G-Cloud Framework and Cloud First policy, government is again removing potential barriers and further enabling public sector organisations to evaluate, procure and consume cloud services.
A potential problem is that while public sector organisations are now clearly encouraged by the new GSCP to make their own decisions rather than being guided by CESG (the independent Technical Authority within government), issues and concerns remain, such as privacy concerns (e.g. US National Security Agency surveillance), sovereignty issues (e.g. US Stored Communications Act) and integrity issues (e.g. the recent OpenSSL Heartbleed bug) which each make some organisations less confident in embracing cloud-based services.

In addition, some Senior Information Risk Officers (SIROs) are also struggling to understand how assets previously classified at Business Impact Level 3 (IL3) or Impact Level 4 (IL4), which may now be classified as OFFICIAL, can be deployed on the same 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. Not all cloud services are created equal, so how public sector organisations can safely select appropriate cloud services is explained, even for the most precious of data assets (e.g. information at IL4).

IN THIS WHITE PAPER

| Introduction to cloud security | 4 |
| New Government Security Classification 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 Skyscape | 19 |
INTRODUCTION TO CLOUD SECURITY

Accredited and secure 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 CloudStore make it easier for the UK public sector to assess the wide range of services available from an extensive list of suppliers. They also provide a quick, compliant and transparent means of awarding a contract and placing an order.

Services offered through the G-Cloud Framework (including the latest iteration, G-Cloud 5) are required to align with the Government Protective Marking Scheme (GPMS), i.e. aligned to Impact Levels (IL) which range from IL0 (no impact or claimed assurance levels), through IL1 and IL2 (the minimum level for commercial, commoditised services for the public sector), to IL3 (designed, delivered and evidenced against HMG guidance, and independently checked and accredited by CESG).

In order to achieve accreditation, the cloud service must be founded upon a suitably scoped Information Security Management System, which should have received certification to the international standard ISO27001 from a recognised UKAS-accredited audit body. Additionally, at IL3, suppliers are required to design, accredit and manage their services using UK government Information Assurance Standards, and to make reference to relevant CESG Good Practice Guides.

Cloud services which have achieved PGA IL2 or PGA IL3 have already been inspected and validated by the CESG Pan Government Accreditor. Services which do not have Pan Government Accreditation require the consuming organisation to invest time and effort on this accreditation activity to provide assurance that the cloud service is appropriately secure — which is in contrast to the government’s Cloud Strategy statement “do it once, do it well and then re-use, re-use, re-use”.

Services offered through the G-Cloud Framework can either be formally pre-accredited by the CESG Pan Government Accradiator (PGA) or unaccredited such that each consuming organisation is responsible for conducting their own formal accreditation (e.g. by their own SIROs).
The launch of the new Government Security Classifications policy (GSCP) on 2 April 2014 introduced a three-tier classification system, which does not directly map onto the previous six tiers within the former GPMS.

Whilst the previous SECRET and TOP SECRET classifications (formerly IL5 and IL6 respectively) remain the same, the remaining categories (IL0 to IL4) have been brought together into a single OFFICIAL classification (as depicted in Figure 1).

A sub-category of OFFICIAL-SENSITIVE has been introduced to enhance certain management and handling controls for data deemed to be especially sensitive. Importantly, OFFICIAL-SENSITIVE does not specify additional mandatory technical controls as the intention is that this data may be hosted on the same platforms as OFFICIAL data.

The GSCP has been introduced to simplify the existing classifications. There are examples of public sector organisations having misinterpreted the previous GPMS to over-engineer solutions in an ill-conceived attempt to address disproportionate risks that were extremely unlikely to ever occur. This would often result in an inefficient non-cloud solution with excessive costs and inadequate agility.

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 now more clearly empowered to properly assess their potential cloud suppliers, to satisfy themselves that risks to their information are properly managed and controlled at every stage of the supplier engagement.

Making an informed decision is of critical importance in ensuring the protection of a public sector organisation’s data. To help inform, a range of guidance published by the government is described in the following section.
GOVERNMENT GUIDANCE FOR SECURITY AND THE CLOUD

Under the previous GPMS, CESG (the independent Technical Authority within government) provided guidance (e.g. Good Practice Guides and Architectural Patterns) and formal accreditation services (e.g. Pan Government Accreditation) to ensure that there is a consistent level of security across the public sector for each Impact Level.

Under the new GSCP, there is more empowerment of each public sector organisation to determine the security controls that they require for the appropriate protection of their data and systems. However, some public sector organisations realise that they are not information security specialists, and many simply don’t know where to start. In recognition of this, Cabinet Office, CESG and Government Digital Services (GDS) have published specific guidance, all outlined below.

Cloud Security Principles

CESG has published a set of guidance centred on 14 Cloud Security Principles 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) and the suitability of the CSP’s staff as determined by appropriate vetting, and so on.

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 that meet the following criteria:

- Ability to demonstrate robust independent assurance (e.g. 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
- Ability to provide differentiated platforms; for example a lower security platform with broad Internet connectivity versus a higher security platform exclusively connected to Government Secure Networks such as PSN.

1 https://www.gov.uk/government/publications/cloud-service-security-principles
Government Service Design Manual

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

You should aim to build services that are appropriately secure, and in practice you will be guided by an assessment of the risks associated with a lapse in the confidentiality, integrity, or availability of your service.

In particular, the Service Design Manual has specific guidance around the approach to security. It promotes the idea of “security as an enabler” rather than being constrained because “security says no”. GDS suggests that “security must be proportionate”, which supports the idea of Cloud Service Providers (CSPs) having differentiated platforms exposed to different risks. For example, many digital solutions are inherently citizen facing and so a cloud service exposed to the Internet is a proportionate risk. Other shared services within government are inherently internal facing and so a PSN-connected cloud service may be preferable because exposure to the Internet might be a disproportionate and unnecessary risk.

The Service Design Manual also urges consumers to “evaluate the privacy risks”. There have been many examples of significant security breaches which 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 consumers can be assured they are compliant with UK laws (e.g. the UK Data Protection Act) and be further assured that privacy is not threatened by foreign legislation (e.g. the US Patriot Act) or other activities by foreign actors (e.g. US National Security Agency surveillance).

G-Cloud and the Government Security Classifications

The G-Cloud Framework (including G-Cloud 5) remains aligned to the previous GPMS (e.g. IL2 and IL3). Under the G-Cloud Framework, suppliers must continue to advertise and fully accredit their cloud services as IL2 and IL3. Hence, on the G-Cloud Framework, consumers will find that the most secure services have PGA IL2 and PGA IL3 badges. Tony Richards, Head of Security & Accreditation for G-Cloud has stated on the government’s “Digital Marketplace” blog that there will be a transition period while G-Cloud develops a new approach that is better aligned to OFFICIAL.

---

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

3 https://digitalmarketplace.blog.gov.uk/2014/03/06/security-accreditation-whats-changing/
When the new classifications go live, buyers will be looking for services that can be used with OFFICIAL data and not for Impact level 2 or 3. We will be advising government buyers to really think about their security requirements and use the Classification Policy Controls Framework and Cloud Security Principles as the basis for their decision-making.

Refer to the section 'Not all clouds are created equal' later in this white paper for more guidance as to the extent to which PGA IL2 and PGA IL3 cloud services are suitable for OFFICIAL data.

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. Aligned to this objective, the Department for Business, Innovation & Skills (BIS) has created and recently launched the new Cyber Essentials Scheme which is designed to help organisations ensure that they are mitigating the risk from internet-based threats that use ‘commodity’ capabilities.

Unlike the other guidance issued by the government and referenced above, the Cyber Essentials Scheme is targeted at smaller enterprises delivering products or services to the UK Public Sector, rather than larger organisations. It is also aimed at internal IT systems rather than platforms used to underpin the provision of a cloud service.

CSPs should achieve independent certification at the Silver Tier against the Cyber Essentials Scheme to further demonstrate the breadth and depth of security that has been implemented across their organisations.

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 and extend the guidance provided by the Cyber Essentials Scheme.

It is advisable that IT systems are aligned with the requirements of the Cyber Essentials Scheme. Service providers should enable each of the five basic controls required by the Scheme and listed below. These control areas are already covered in existing frameworks such as the ISO27001 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 Bridge which further controls the level of internet access into this environment.

2. **Secure configuration** — the service should be secure by default. The customer’s self-managed firewall pre-configured to block all access until they specify traffic which they explicitly wish to allow to pass. The supplier should also provide a number of operating system images within its Service Catalogue which have also been designed as secure by default.

---

3. **User access control** — the management portal should provide full Role Based Access Control (RBAC) which allows customers to control which of their users have access to 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 as they have 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 which gives them full permissions to apply patches. The supplier should also make certain patch repositories available within a higher security domain to further assist with patch deployment.

---

**CERT-UK**

CERT-UK\(^5\) is the UK Computer Emergency Response Team which was recently launched to work closely with industry, government and academia to enhance the UK’s level of cyber resilience.

Like the Cyber Essentials Scheme, CERT-UK is part of the National Cyber Security Strategy and is responsible for:

- National cyber security incident management
- Support to critical national infrastructure companies to handle cyber security incidents
- Promoting cyber security situational awareness across industry, academia and the public sector
- Providing 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. As part of CESG Pan Government Accreditation, some CSPs have already implemented protocols to work with GovCERT. These same protocols can be extended to support initiatives such as sector-based WARP\(\)s (Warning and Advisory Reporting Points) and can facilitate membership of the CERT-UK Cyber Information Sharing Partnership (CISP). Although CERT-UK focuses on the management of cyber security incidents, they do aggregate best practice advisories such as the ‘10 Steps to Cyber Security’\(^6\) published by BIS and the ‘20 Critical Controls’\(^7\) published by the Centre for the Protection of National Infrastructure (CPNI).

---


TRANSITIONING TO THE NEW SECURITY CLASSIFICATIONS

CESG has published specific guidance on how to use the Cloud Security Principles when making risk management decisions⁸. Consistent with CESG’s guidance, Cabinet Office also recommends that public sector organisations continue to adopt good Risk Assessment and Risk Management processes (e.g. IS1/IS2) in order to evaluate the risks to the information assets. Under IS1/IS2, it remains appropriate to reference the Business Impact Level tables. Hence, consumers who have already determined the business impact of a loss of confidentiality, integrity and availability (denoted as IL2/IL3/IL4) may find this section useful in considering what they might look for under the OFFICIAL classification of the GSCP.

Consumers should also consider the legal jurisdiction of the cloud service they are evaluating. Many cloud services operate outside UK jurisdiction in territories such as North America, mainland European Union, etc which may pose an additional risk to the confidentiality (e.g. privacy) and availability of the service being consumed. An example of this is the 2014 case where a US Court ordered Microsoft to release data even though it was held in Ireland⁹.

Transitioning from IL2 to OFFICIAL

IL2 assets should be relatively simple to transition to the OFFICIAL classification under the GSCP. Under the previous GPMS, cloud services suitable for IL2 were required to adhere to commercial best practice as evidenced by an appropriately scoped ISO27001 certification from a UKAS recognised audit body. Under the new GSCP, the OFFICIAL tier has a similar requirement.

Consumers should seek assurance that CSPs have actually implemented and operate commercial good practice controls. The G-Cloud Pan Government Accreditation (PGA) by CESG is a useful benchmark in this respect. There are many cloud services which have achieved formal CESG PGA accreditation at IL2. Cloud services which have not achieved this relatively low bar should be thoroughly scrutinised.

Transitioning from IL3 to OFFICIAL

IL3 assets have a more difficult transition to the OFFICIAL classification under the Government Classification Scheme. Under the previous GPMS, cloud services suitable for IL3 were expected to adhere to CESG Good Practice (such as limiting connectivity to a trusted community of users such as GSI). The suitability of cloud services for IL3 was evidenced by G-Cloud Pan Government Accreditation and PSN Accreditation; both involve extensive documentation, auditing and technical testing by independent security specialists. Under the new GSCP, the OFFICIAL tier no longer enforces these requirements.

Consumers should seek assurance that CSPs have actually implemented and operate appropriate CESG good practice controls (e.g. protective monitoring that complies with Good Practice Guideline 13) that remain relevant regardless of the change to the new GSCP. The G-Cloud Pan Government Accreditation (PGA) or PSN Accreditation (PSNA) at IL3 is a desirable benchmark in this respect.

---


⁹ http://www.bbc.co.uk/news/technology-27191500
There are comparatively few cloud services which have achieved CESG PGA or PSN accreditation at IL3. This makes it tempting to consider using non-accredited or self-accredited cloud services so public sector organisations need to carefully evaluate the risks of doing this.

Consumers should consider the legal jurisdiction of the cloud service they are evaluating (as mentioned above). Many cloud services operate outside UK jurisdiction which may pose an additional risk to the confidentiality (e.g. privacy) and availability of sensitive assets at IL3. It is essential that cloud providers host and manage their cloud service from within the UK for assets previously classified at IL3 or above but now classified as OFFICIAL.

Finally, a subset of assets at IL3 (e.g. a register of vulnerable adults) could be considered to be managed using the OFFICIAL-SENSITIVE sub-category. Under this sub-category, information should be more tightly restricted on a strict ‘need to know’ basis. One way to achieve this is to host these assets on a cloud platform which is only connected to the closed community of PSN users rather than openly connected to the Internet. This is often termed a Community Cloud rather than a Public Cloud. Some CSPs offer both types of cloud service; those exposed to the Internet and those directly connected only to Government Secure Networks (such as GSI, PSN, N3, etc). For services connected to the PSN, consumers should look for the enhanced assurance provided by independent PSN Accreditation at IL3.

### Transitioning from IL4 to OFFICIAL

IL4 assets have the most difficult transition to the OFFICIAL classification under the Government Classification Scheme. Under the previous GPMS, cloud services suitable for IL4 were expected to adhere to even more onerous controls related to people, processes and technology than compared with IL3.

Given the potential impact related to the confidentiality, integrity and/or availability of these data assets, it is essential that consumers look for the following over and above the relatively low baseline controls allowed by the OFFICIAL tier:

1. **UK Jurisdiction** — it is critical that data assets remain within the UK, hosted in secure UK data centres and operated by UK security cleared staff. The risk of such sensitive data being subject to foreign legislation (e.g. the US Patriot Act) or foreign surveillance is intolerable for most risk owners.

2. **Community Cloud** — it is essential that data assets at IL4 remain tightly controlled and shared only across Government Secure Networks such as PSN, N3, etc. Hosting these 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 Community Cloud platforms and Public Cloud platforms in order to support digital initiatives such as enabling citizens to access these systems securely.
NOT ALL CLOUDS ARE CREATED EQUAL

With the change from the existing GPMS to the new GSCP, the government has empowered public sector organisations to accelerate their consumption of cloud services by silencing the "Security says no" mentality that was sometimes an unfortunate feature of the previous GPMS.

However, it is essential that public sector organisations don't simply move from one extreme ("Security says no") to the other by assuming that all cloud services are created equal.

Some cloud services will provide all of the security principles, while others only a subset… Some service providers will be able to offer higher levels of confidence in how they implement the different security principles. — Cloud Security Principles, CESG

As recognised by CESG, there are many cloud services that will provide only a subset of the core security principles, and an even greater number of cloud services that will provide the light assurance of self-certification and offer no independent validation or measurement as to how well, or how poorly, the security principles are being implemented and operated.

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

1. **Accredited Public Cloud services**: cloud services which have achieved CESG PGA IL3

2. **Assured Public Cloud services**: cloud services which have achieved CESG PGA IL2

3. **Unassured cloud services**: cloud services which have not achieved CESG Pan Government Accreditation, for example global cloud services such as Amazon Web Services (AWS), Dropbox, etc

Aligned to Cabinet Office guidance, Figure 2 depicts the varying extent of how different categories of cloud services meet the requirements of systems classified as OFFICIAL. It can be seen that only 'Accredited Cloud Services' (as evidenced by CESG PGA IL3) are suitable for all OFFICIAL information. 'Assured Cloud Services' (as evidenced by CESG PGA IL2) is expected to be suitable for most OFFICIAL information. 'Unassured Cloud Services' are said to be suitable for only some OFFICIAL information.

The value of CESG PGA Accreditation for Assured OFFICIAL (IL2)

Skyscape Cloud Services has built a truly unique cloud services platform; a platform which is entirely UK sovereign, with two geographically separate UK datacentres operated by UK-based security cleared staff. Skyscape has always held information security and transparency as core values, further evidenced by formal independent certification from LRQA against the international standards for information security (ISO27001), IT service management (ISO20000) and quality management (ISO9001). Further, Skyscape was amongst the very first to achieve CESG Pan Government Accreditation at IL2 and also PSN Accreditation which independently validates the effectiveness of the systems and controls that Skyscape has implemented.

---

All of this is provided exclusively to UK public sector consumers. All Skyscape cloud services are provided on a true utility model; no-upfront costs, no extended lead time, no minimum contract term. Simply, genuine usage-based billing (per virtual machine per hour or per GB per month).

There is an alternative to the global clouds run by Amazon Web Services, Google and Microsoft. Beware of supplier self-affirmations; always seek independent, traceable verification.

**The value of PSN Accreditation for Elevated OFFICIAL (IL3)**

In addition to our Assured OFFICIAL (IL2) platform, Skyscape operates a second platform called Skyscape Elevated OFFICIAL (IL3) which benefits from being a true Community Cloud.

Whereas the Skyscape Assured OFFICIAL (IL2) cloud platform is directly connected to the Internet, the Skyscape Elevated OFFICIAL (IL3) cloud is connected exclusively to Government Secure Networks such as PSN, GSI and N3.

This provides consumers with true cloud services within a secure, closed community of likeminded users. This can be considered a safe environment for solutions such as shared services where it is essential that sensitive information assets are never vulnerable to untrusted Internet traffic and unknown organisations.

In this context, consumers can draw additional assurance from the Pan Government Accreditation and PSN Accreditation that Skyscape’s cloud services hold at IL3 which are both G-Cloud Pan Government Accredited and also PSN Accredited.

*Figure 2. How accredited, assured and unassured clouds meet OFFICIAL requirements*
Comparing cloud platforms using Cloud Security Principles

Under the new GSCP, consumers are able to select general Public Cloud platforms if they deem the security that they offer is appropriate for their data. The table below shows how the Skyscape cloud platforms compare with a typical Public Cloud platform:

<table>
<thead>
<tr>
<th>Security Principle</th>
<th>Typical Public Cloud</th>
<th>Skyscape Assured OFFICIAL cloud (IL2)</th>
<th>Skyscape Elevated OFFICIAL cloud (IL3)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NIST Cloud Model</strong></td>
<td>Public Cloud</td>
<td>UK Sovereign Public Cloud (designed for UK Public Sector)</td>
<td>Community Cloud for UK Public Sector</td>
</tr>
</tbody>
</table>

**Security and Assurance**

<table>
<thead>
<tr>
<th>Data Centre Locations</th>
<th>Varies — typically North America or continental Europe</th>
<th>Both data centres in the UK separated by more than 100 kilometres</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location of Service Management</td>
<td>Varies - typically North America, continental Europe or continental Asia</td>
<td>Entirely within the UK from two secure sites which are both Pan Government Accredited to IL3</td>
</tr>
<tr>
<td>Security of Data Centre</td>
<td>Varies</td>
<td>Both data centres assessed by CESG Pan Government Accreditors as part of Skyscape’s PGA IL3 accreditation and independently capable of achieving IL5 status</td>
</tr>
<tr>
<td>Vetting of Staff</td>
<td>Varies</td>
<td>All employees are subject to security clearance. All operational staff with access to the Skyscape platform undergo a formal Security Check (SC) and in some cases Non-Police Personnel Vetting (NPPV). All employees have signed the Official Secrets Act and benefit from regular Information Security education.</td>
</tr>
<tr>
<td>Protective Monitoring</td>
<td>No</td>
<td>Skyscape 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.</td>
</tr>
</tbody>
</table>
### Security and Assurance (cont.)

<table>
<thead>
<tr>
<th>Security Principle</th>
<th>Typical Public Cloud</th>
<th>Skyscape Assured OFFICIAL cloud (IL2)</th>
<th>Skyscape Elevated OFFICIAL cloud (IL3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pan Government Accredited (IL2)</td>
<td>No</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>PSN Accredited (IL2)</td>
<td>No</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Pan Government Accredited (IL3)</td>
<td>No</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>PSN Accredited (IL3)</td>
<td>No</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Suitable UKAS ISO27001, ISO20000 and ISO9001 certifications</td>
<td>Not usually</td>
<td>Yes (LRQA)</td>
<td>Yes (LRQA)</td>
</tr>
<tr>
<td>Cloud Security Alliance (CSA) membership</td>
<td>Not usually</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cloud Essentials Scheme</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Connectivity Options

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct resilient Internet connectivity</td>
<td>Yes</td>
<td>Yes</td>
<td>No (indirect/controlled via Cross Domain Bridge)</td>
</tr>
<tr>
<td>CPA Foundation Grade VPN support</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PSN connectivity</td>
<td></td>
<td>PSN ‘Assured’ Service</td>
<td>PSN ‘Protected’ service</td>
</tr>
<tr>
<td>N3 connectivity</td>
<td></td>
<td>Yes</td>
<td>Yes (with appropriate technical controls)</td>
</tr>
<tr>
<td>Private Circuit Support</td>
<td>No</td>
<td>Yes (CAS-T)</td>
<td>Yes (CAS-T with CPA encryption)</td>
</tr>
</tbody>
</table>

The table above shows that typical Public Cloud platforms are not able to provide either the breadth or depth of security that Skyscape Cloud Services provides as standard. Skyscape services have been independently and repeatedly inspected under CESG G-Cloud Pan Government Accreditation, PSN Accreditation and certification under commercial schemes such as ISO27001 and CSA STAR. All Skyscape services are available on the same commercial terms as many generic Public Cloud services, yet as the table above shows, the Skyscape platform is designed to address a much wider range of UK public sector specific challenges.
Figure 3 shows the relative positioning of CSPs when considering value (y-axis) and appropriate security (x-axis).

Providers that score well against the security axis (typically long-term suppliers to government) often do not provide best value as they typically require upfront investment, minimum contract term, monthly billing (regardless of usage), etc.

Public Cloud providers that score well against the value axis often do not provide sufficient levels of security appropriate for UK public sector organisations (e.g. misaligned with Cloud Security Principles, for example offshore data centres, offshore service centres, unvetted staff, etc).

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

*Figure 3. Relative positioning of CSPs: value vs security*
Skyscape has introduced “Optimised for OFFICIAL”, a product mark designed for UK public sector organisations to give them assurance the cloud services bearing this mark are closely aligned to CESG Cloud Security Principles.

*Figure 4. The Skyscape ‘Optimised for OFFICIAL’ product mark*

Each of Skyscape’s cloud services will bear this mark along with selected products and services from over 100 Skyscape partners. Skyscape partners provide value-add cloud services ranging from Software-as-a-Service (SaaS) offerings (powered by Skyscape) to specialist cloud services such as management, transition and transformation services.
SUMMARY

Based on the government guidance described in this document, Skyscape Cloud Services 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 United Kingdom, hosted in secure UK data centres and operated by a UK company. Skyscape believes the risk of sensitive data being subject to foreign legislation (e.g. the US Patriot Act) or foreign surveillance is a significant issue for many risk owners.

☑ 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-up to the Official Secrets Act.

☑ Broad Connectivity — the cloud services platform should be resiliently connected to the Internet as well as Government Secure Networks such as PSN, N3 and GSI. The cloud service should be formally PSN Accredited so that it a recognised PSN compliant service.

☑ GPG13 Protective Monitoring — the cloud service should benefit from robust Protective Monitoring. Protective Monitoring should be 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 is safely and exclusively connected to Government Secure Networks (e.g. a Community Cloud).

☑ Cross Domain Bridge — recognising that there will be some OFFICIAL systems which are less secure than others, public sector organisations should require a Cross Domain Bridge which supports PGA-approved scenarios to facilitate controlled citizen access to sensitive data sets.

☑ Independent Validation — do not trust self-accreditation; seek cloud services which have extensive independent validation and testing by recognised authorities (such as CESG).

☑ Cloud Security Principles — look for cloud services which have implemented each of the 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.
Skyscape Cloud Services has developed a range of cloud services designed specifically for the UK public sector, to help increase efficiencies, reduce costs, significantly improve procurement times and increase transparency. Our services are easy to adopt, easy to use and easy to leave to ensure that our customers remain in complete control, with minimum risk, reassured by the fact Skyscape’s services are Pan Government Accredited (PGA) up to IL3.

Skyscape’s full offering consists of IaaS, PaaS and SaaS products:

- **IaaS** — seven offerings around Compute and Storage on demand
- **SaaS** — 17 offerings around messaging and document management
- **PaaS** — based upon Cloud Foundry

All of Skyscape’s UK sovereign cloud computing services are hosted in one (or both) of our highly resilient Tier 3 UK data centres in Farnborough and Corsham. Skyscape services are delivered with leading technologies from Skyscape Alliance Partners: QinetiQ, VMware, Cisco, EMC and Ark Data Centres. The Cloud Alliance also provides a collaborative resource which drives innovation and technical product development, helping to continually improve Skyscape’s offering to meet the needs of the UK public sector.

Skyscape is focused on providing cloud services in a more agile, secure and cost-effective manner. We strive to deliver solutions that harness technology as a way to facilitate the changes that are needed to streamline processes and reduce costs to support the UK public sector and, ultimately, UK citizens and taxpayers.

**MORE INFORMATION**

For further information about Skyscape Cloud Services and how we can help you, please send an email to info@skyscapecloud.com