Seeding the Global Public Sector Cloud:
Part II – The UK's Approach as Pathfinder for Other Countries[1]

Abstract: This is the second of a two part paper that assesses current trends in the adoption of public sector cloud computing by governments around the world. Part I briefly overviewed the potential for and inhibitors to government cloud growth, focusing on security and risk management concerns and suggesting a role for ISO standards, especially ISO 27001 and ISE 27018, in effectively addressing these inhibitors. Part II focuses on the structured approaches to cloud adoption taken by a number of countries including the UK, and suggests that countries looking to develop their public sector clouds but without wishing to reinvent this particular wheel could validly start from the UK's approach as a pathfinder.

The progress of public sector cloud computing has faced headwinds around the world arising from concerns principally about security and how practically and effectively to manage risk. Addressing these concerns will enable the potential of the global public sector cloud to start to be fulfilled, a step-change that has been widely forecast to take place over the next few years: Part I of this paper referenced forecasts that the public sector cloud is set to account for more than half global software and storage spending growth by 2018 and that US federal cloud spending is predicted to grow from $3bn today to $6.5bn by 2019.[2]

Part I suggested that international standards, particularly ISO 27001[3] on information security management systems and ISO 27018[4] on the protection of personally identifiable information (**PII**) in the cloud, provide particularly useful tools to unlock growth in global public sector cloud uptake through demonstrable and demonstrated procedures designed to assess, certify, benchmark and audit achievement of cloud security standards.

Accreditation to these standards is a key *output* for demonstrating risk management outcomes, and this in turn depends and is built on substantive elements of a model public sector cloud computing security framework as *inputs*. This part of the paper proposes that an effective cloud security framework model encompasses the following substantive inputs:

- an approach *led from the centre and applied consistently* across government;
- on a foundation of *robust data classification*;
- which is *transposed effectively to the cloud*; and
- which enables baseline *cloud security requirements to be mapped to the classification*.

We suggest that combining substantive cloud security framework *inputs* constructed this way with effective use of security management international standards at the procedural level as *outputs* can provide government ICT (information and communications technology) functions with a route map to effective public sector cloud adoption. Following a brief review of government cloud adoption to date in a number of geographies, we suggest that the UK's approach to these issues can validly serve as a pathfinder for countries looking to develop their public sector clouds who do not necessarily want to reinvent this particular wheel.

---

[1] Richard Kemp, Kemp IT Law, London, richard.kemp@kempitlaw.com. All footnoted sources were accessed between 23 July and 6 October 2015

[2] Sources: *IDC Worldwide and Regional Public Cloud IT Services 2014 – 2018 Forecast* and *Deltek Federal Industry Analysis* cited in Forbes Insights, *From promise to Reality: How Local, State and Federal Government Agencies Achieve Results from the Cloud* (May 2015) available at http://www.forbes.com/forbesinsights/microsoft_govt_cloud/index.html

[3] See http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

[4] See http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498

A Sampling of Approaches: The US, ENISA and Germany

In the USA, the US Chief Information Officer in December 2010 published a *25-Point Implementation Plan to Reform Federal IT Management*,[5] one element of which was to adopt a Cloud First policy, articulated in the February 2011 *Federal Cloud Computing Strategy* (**FCCS**).[6] The FCCS is supported and complemented by a number of other US government initiatives and programs,[7] including the Federal Risk and Authorisation Management Program (**FedRAMP**).[8] FedRAMP was established in December 2011 to provide a standardised, centralised approach to assessing and authorising cloud computing services and products. As at June 2015,[9] there were reported to be around forty providers, products and services certified under FedRAMP.

Figure 1: ENISA Security Framework based on 'Plan → Do → Check → Act' Lifecycle

Phase	Security Activity	Security Step
A. Plan	a) Risk profiling	1. Identify services to cloudify
		2. Select security dimensions[10]
		3. Evaluate individual impact to these dimensions
		4. Determine global risk profile
	b) Architectural model	5. Decide on deployment – service model[11]
	c) Security & privacy requirements	6. Establish security requirements
B. Do	d) Security controls	7. Selection of security controls
	e) Implementation deployment and accreditation	8. Formalisation and implementation of selected security controls
		9. Cloud service suitability ex ante verification to provide sufficient assurance
		10. Start service execution
C. Check	f) Log/monitoring	11.Periodically check that security controls are in place and being followed
	g) Audit	12. Verification that the defined/contracted levels of security are fulfilled
D. Act	h) Change management	13. Implementation of remedies & improvement to security framework/approach
	i) Exit management	14. Contract termination, return of data to customer and data deletion

[5] Available at https://cio.gov/resources/document-library/

[6] Available at www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf

[7] See Congressional Research Service Report *Overview and Issues for Implementation of the Federal Cloud Computing Initiative: Implications for Federal Information Technology Reform Management* (January 2015) for a discussion of these initiatives and programmes.

[8] http://www.fedramp.gov/

[9] See for example Bill Glanz in FedRAMP411 *Goodrich Opens up at Cloud Brainstorm* (24 June 2015) available at http://www.fedramp411.com/article/Goodrich

[10] Based on availability, integrity and confidentiality

[11] Whether public, private, community, cloud

At EU level, ENISA (the EU Agency for Network and Information Security) in February 2015 published its report *Security Framework for Governmental Clouds*[12], which examined four selected public sector cloud use cases in:

- *Estonia*: planned public/private cloud IaaS/PaaS/SaaS in public administration services;
- *Greece*: deployed public cloud IaaS in educational and academic community;
- *Spain*: deployed private cloud SaaS in general and regional administration services; and
- *UK*: deployed public cloud IaaS/PaaS/SaaS in services of the public sector.

Based on these uses cases, the ENISA paper proposed a security framework modelled on four lifecycle phases, nine security activities and fourteen security steps, as set out in Figure 1 above.

Germany's Federal Ministry of Economics and Technology in November 2010 published its *ICT Strategy of the German Federal Government: Digital Germany 2015*[13] and has since launched a Trusted Cloud Technology Programme[14] 'to support the development of innovative, secure and legally compliant cloud solutions'. Germany's Cloud Computing Action Programme was aimed particularly at the public sector with a view to researching the cloud, developing an innovative security framework around security, legal and standards certification considerations and influencing international developments.

The UK Approach: Driving Public Sector Entities to the Cloud

As mentioned above, the UK Government (which, as with most states is the biggest buyer and user of ICT in the country[15]) has examined and assessed each element of its cloud security framework and published its work in a comprehensive and comprehensible articulation of the substantive organising input elements which an effective cloud security framework model is shown to encompass. The guidance and other related documentation published by the UK Government is summarised in the Annex to this part of the paper, along with the publication's date, URL and status as at end July 2015.

The whole framework is freely publicly available and has been published from central government – whether the UK Cabinet Office (the department that leads the Government's efforts to ensure joined up and effective implementation of policy) the CESG (the Communications-Electronic Security Group within GCHQ, the Government Communications HQ) or the top echelons of the UK Civil Service. This transparency is designed to ensure consistency of approach across government and to avoid the major risk of fragmentation that would that would otherwise arise with bespoke requirements and implementations. The framework is based on ICT strategy work in 2011 at the start of the last UK administration[16] and the *Government Security Policy Framework* of April 2014 (Annex, point 2.1).

---

[12] Available at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/governmental-cloud-security/security-framework-for-govenmental-clouds

[13] Press Release available at http://www.bmwi.de/EN/Press/press-releases,did=373072.html

[14] http://www.microsofttranslator.com/bv.aspx?from=&to=en&a=http%3A%2F%2Fwww.trusted-cloud.de%2F

[15] In the UK in Q1 2015, total public sector employment stood at 5.372m, 17.3% of total UK employment of 31.053m. Of the 5.372 million, 1.589m (29.6%) were employed in the National Health Service; 1.514m in education (28.2%); 1.042m (19.4%) in public administration; 0.254m (4.73%) in the police service; 0.252m (4.69%) in 'other health and social work'; 0.161m in the armed forces (3.0%); and 0.53m (9.9%) in 'other public sector'. See http://www.ons.gov.uk/ons/rel/pse/public-sector-employment/q1-2015/stb-pse-2015q1.html

[16] See the documents referenced at Annex, points 1.1 and 1.2, now replaced by the *Government Service Design Manual* and the *Digital by Default Service Standard* of June 2015 at Annex, points 1.4 and 1.5, although the *Government Cloud Strategy*, also of 2011, has not been withdrawn.

UK Data Classification: The Key to Unlocking the Cloud

A structured approach to data classification is a critical tool for managing an organisation's data assets. Data subsists in one of three states (at rest, in process, in transit), can be either structured or unstructured and is subject to access control based on authentication (verifying that the user is who they say they are) and authorisation (providing an authenticated user with the ability to access the data concerned). A particular data classification will also depend on data compliance considerations (like the jurisdictions of the origin and domicile of the data, and statutory, contractual and other legal constraints) and require a terminology model articulating levels of classification sensitivity. In the words of a 2014 Microsoft white paper, *Data Classification for Cloud Readiness*:[17]

> "Data classification provides one of the most basic ways for organizations to determine and assign relative values to the data they possess. The process of data classification allows organizations to categorize their stored data by sensitivity and business impact in order to determine the risks associated with the data. After the process is completed, organizations can manage their data in ways that reflect its value to them instead of treating all data the same way. Data classification is a conscious, thoughtful approach that enables organizations to realize optimizations that might not be possible when all data is assigned the same value."

Driven in large part by the digitisation of UK public sector workloads, the UK Government in 2013 carried out a major overhaul of the way in which it classified data. This led to the *Government Security Classifications* guidance published in April 2014 (Annex, point 3.1) when the longstanding five level classification that then applied[18] was replaced with a new three level system of OFFICIAL → SECRET → TOP SECRET. The reduction from five to three classes was critical in respect of the new OFFICIAL category, where, in the 'key points' section of its two page October 2013 briefing to suppliers about the new classifications (Annex, point 3.2), the Cabinet Office said:

> "The OFFICIAL classification covers up to *ninety percent of Public Sector business*, including most policy development, service delivery, legal advice, personal data, contracts, statistics, case files, and administrative data.
>
> - Security controls at OFFICIAL are based on good, commercially available products, in the same way that the best-run businesses manage their sensitive information.
> - Particularly sensitive OFFICIAL information will be controlled through local handling arrangements that reinforce the 'need to know' principle (emphasis added)."

Page 7 of the UK Government Security Classifications highlights examples of what is considered OFFICIAL, including:

> "
> - The day to day business of government, service delivery and public finances.
> - Routine international relations and diplomatic activities.
> - Public safety, criminal justice and enforcement activities.
> - Many aspects of defence, security and resilience.
> - Commercial interests, including information provided in confidence and intellectual property.
> - Personal information that is required to be protected under the Data Protection Act (1998) or other legislation (e.g. health records)."

A data classification framework is not only about placing data in the appropriate sensitivity category, but also about associating the right level of security controls with that data. The UK approach dictates that OFFICIAL information:

---

[17] https://technet.microsoft.com/en-US/security/jj554736

[18] UNCLASSIFIED → RESTRICTED → CONFIDENTIAL → SECRET → TOP SECRET

> "must be secured against a threat model that is broadly similar to that faced by a large UK private company"[19]

with levels of security controls that:

> "are based on good, commercially available products in the same way that the best-run businesses manage their sensitive information".[20]

The wide coverage of the OFFICIAL classification, equating it to information held in the private sector and the repeated admonitions by UK policy makers to avoid over classifying government data were all very intentional. These conscious policy decisions represent ground-breaking and profound change and were implemented to enable public sector entities to more easily reap benefits from deploying commodity cloud solutions:

> "This change in approach will enable the public sector to take advantage of a wider range of modern, lower cost (commodity) security products rather than defaulting to expensive, bespoke or augmented technologies."[21]

When viewed in conjunction with the UK G-Cloud marketplace, it is clear that the developments related to the OFFICIAL category (including its wide scope of coverage and the statement that such information should be secured consistent with "good commercial practice") were intended to convey a message that the commodity cloud services available through the G-Cloud marketplace are suitable for handling OFFICIAL information

This new classification paves the way for the application of public cloud services, under suitable security conditions, to most workloads of OFFICIAL data in the UK, which the government itself states covers nine tenths of the UK public sector data estate[22]. When, at scale, public cloud services are estimated to cost one-tenth of services delivered over a smaller scale private cloud, it can be appreciated how big an enabler this robust data classification is to the development of the public sector cloud in the UK.

Other countries grappling with the issues of categorisation and classification include Estonia, Greece and Spain (as mentioned in Annex A/B[23] to the February 2015 ENISA *Security Framework for Government Clouds* referred to above). In response to the questions 'do you have a National Information Asset classification scheme?' and 'how do you classify government assets?':

- *Estonia's* response was to say that 'the owner of data determines the information security level needed' and that security risk is categorised as LOW, MEDIUM or HIGH (Annex A/B, pages 22 and 23;
- the response of *Greece* was to classify four types of data (public, internal, confidential and special) by reference to the information security required and with three security levels applicable to cloud services (LOW, MEDIUM, HIGH) (pages 22 to 24); and

[19] *Government Security Classifications* (April 2014) at Annex, point 3.1, page 17

[20] *Government Security Classifications Supplier Briefing* (October 2013) at Annex, point 3.2

[21] Page 5, FAQ 2 – Managing Information Risk at OFFICIAL at Annex, point 3.5

[22] For the other 10 percent (i.e. SECRET and TOP SECRET information) the classification threshold is particularly high. 'SECRET' includes 'very' sensitive information whose compromise 'would be likely to directly threaten an individual's life, liberty or safety…' 'TOP SECRET' includes 'exceptionally' sensitive information whose compromise 'would be likely to lead directly to widespread loss of life …' (pages. 8 and 9 of the *Government Security Classifications* at Annex, point 3.1)

[23] Available at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/governmental-cloud-security/security-framework-for-govenmental-clouds

- *Spain* has 'three security levels (LOW, INTERMEDIATE, HIGH) in which systems can be classified, and those levels guide the selection of security controls' (page 1).

In July 2015, *Indonesia* published a draft policy[24] addressing security risk management on the basis of classification not of data but of electronic systems (defined as 'a series of electronic devices and procedures' for a wide range of activities in relation to electronic information), categorised as STRATEGIC, HIGH or LOW.

Whilst there may be differences of view as to whether the preferable classification basis is at the data or system level, all these examples show the governments concerned not treating everything the same, and addressing questions of taxonomy in a structured way based on perceived risk, typically on a three tier basis.

Security Requirements for Official Data

The data classification, which is general and applies across government, has then to be transposed to the cloud for mapping of cloud security standards. Here, the UK Government has published an *Introduction to Cloud Security Guidance*, *Summary of Cloud Security Principles* and guidance on *Cloud Security Principles Implementation* (Annex, points 4.2, 4.1 and 4.4), along with more specific cloud security guidance on risk management, separation, IaaS and standards and definitions (Annex, points 4.3, 4.5, 4.6 and 4.7). The UK's fourteen Cloud Security Principles, their description and why they are important are summarised below in Figure 2.

Figure 2: Table Summarising the UK Cloud Security Principles[25]

Cloud Security Principle /Description	**Why this is important: if this principle is not implemented then -**
1. **Data in transit protection** Consumer data transiting networks should be adequately protected against tampering and eavesdropping via a combination of network protection and encryption.	The integrity or confidentiality of the data may be compromised whilst in transit.
2. **Asset protection and resilience** Consumer data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.	Inappropriately protected consumer data could be compromised which may result in legal and regulatory sanction, or reputational damage.
3. **Separation between consumers** Separation should exist between different consumers of the service to prevent one malicious or compromised consumer from affecting the service or data of another	Service providers cannot prevent a consumer of the service affecting the confidentiality or integrity of another consumer's data or service.
4. **Governance framework** The service provider should have a security governance framework that coordinates and directs their overall approach to the management of the service and information within it.	Any procedural, personnel, physical and technical controls in place will not remain effective when responding to changes in the service and to threat and technology developments.
5. **Operational security** The service provider should have processes and procedures in place to ensure the operational security of the service.	The service can't be operated and managed securely in order to impede, detect or prevent attacks against it.

[24] See http://kominfo.go.id/index.php/content/detail/5129/Siaran%20Pers%20No.54-PIH-KOMINFO-07-2015%20tentang%20Uji%20Publik%20Rancangan%20Peraturan%20Menteri%20mengenai%20Sistem%20Manajemen%20Pengamanan%20Informasi/0/siaran_pers#.VhQUfqSFOUn. For an English translation, the writer used Bing Translator: http://www.microsofttranslator.com/bv.aspx?from=&to=en&a=http%3A%2F%2Fkominfo.go.id%2Findex.php%2Fcontent%2Fdetail%2F5129%2FSiaran%2BPers%2BNo.54-PIH-KOMINFO-07-2015%2Btentang%2BUji%2BPublik%2BRancangan%2BPeraturan%2BMenteri%2Bmengenai%2BSistem%2BManajemen%2BPengamanan%2BInformasi%2F0%2Fsiaran_pers%23.Vec55jZREwy

[25] From the document at Annex, point 4.1, *Overview - Summary of Cloud Security Principles*

6. **Personnel security** Service provider staff should be subject to personnel security screening and security education for their role.	The likelihood of accidental or malicious compromise of consumer data by service provider personnel is increased.
7. **Secure development** Services should be designed and developed to identify and mitigate threats to their security.	Services may be vulnerable to security issues which could compromise consumer data, cause loss of service or enable other malicious activity.
8. **Supply chain security** The service provider should ensure that its supply chain satisfactorily supports all of the security principles that the service claims to implement.	Tt is possible that supply chain compromise can undermine the security of the service and affect the implementation of other security principles.
9. **Secure consumer management** Consumers should be provided with the tools required to help them securely manage their service.	Unauthorised people may be able to access and alter consumers' resources, applications and data.
10. **Identity and authentication** Access to all service interfaces (for consumers and providers) should be constrained to authenticated and authorised individuals	Unauthorised changes to a consumer's service, theft or modification of data, or denial of service may occur.
11. **External interface protection** All external or less trusted interfaces of the service should be identified & have appropriate protections to defend against attacks through them.	Interfaces could be subverted by attackers in order to gain access to the service or data within it.
12. **Secure service administration** The methods used by the service provider's administrators to manage the operational service should be designed to mitigate any risk of exploitation that could undermine the security of the service.	An attacker may have the means to bypass security controls and steal or manipulate large volumes of data.
13. **Audit information provision to consumers** Consumers should be provided with the audit records they need to monitor access to their service and the data held within it	Consumers will not be able to detect and respond to inappropriate or malicious use of their service or data within reasonable timescales.
14. **Secure use of the service by the consumer** Consumers have certain responsibilities when using a cloud service in order for this use to remain secure, and for their data to be adequately protected.	The security of cloud services and the data held within them can be undermined by poor use of the service by consumers.

These fourteen Cloud Security Principles are particularly useful as a concise but still comprehensive statement of requirements. They have been taken up by the supplier community, and large international cloud service providers like Amazon and Microsoft have published materials[26] based on them and also linking them to ISO 27001 in order to assist UK public sector customers in making cloud service buying decisions on consistently with the mandated requirements. Adoption in this way by the provider community in the UK also increases their readiness elsewhere and paves the way for more general application of the principles in different geographies.

Effective transposition of the data classification to the cloud environment in this way therefore enables baseline cloud security requirements to be mapped to the classification through these cloud security principles. The security framework embodied by the UK Government documentation suite listed in the Annex explains the ways in which public sector entities can then determine and demonstrate compliance with the principles. These include:

(i) cloud service provider assertion;
(ii) cloud service provider contractual commitment;
(iii) third party certification;
(iv) independent testing; or

[26] For Amazon see: https://blogs.aws.amazon.com/security/post/Tx31CWNXWOP2J09/Using-AWS-in-the-Context-of-CESG-UK-s-Cloud-Security-Principles. For Microsoft see: http://www.microsoft.com/en-gb/enterprise/it-trends/cloud-computing/articles/14-points.aspx#fbid=MyGgwF29ZRe

(v) a mix of one or more of these.

In a world where authorities are sceptical (appropriately so in some cases) about cloud service providers' self-asserted statements [(i)] and even contractual commitments [(ii)], and independent testing [(iii)] may well be disproportionate, the value of third party certification [(iii)] - particularly where as in the case of ISO 27001 it aligns with the cloud security principles listed above – is real and, as explained in Part I of this paper, able to operate at the scale of the public sector cloud on a global basis.

Conclusions

The UK's approach is transparent and consistent, based on robust data classification and transposed to the cloud, to which a comprehensive set of security requirements have then been mapped through the cloud security principles. This practical approach to data classification, where the UK envisages that the OFFICIAL tier will account for up to ninety percent of government data, is coupled with an equally pragmatic appreciation that appropriate security controls will reflect good commercial practice. These substantive elements of the UK's public sector cloud computing security framework *inputs* can in turn be combined with demonstrable and demonstrated procedures designed to assess, certify, benchmark and audit achievement of *output* cloud security standards based on ISO 27001 and ISO 27018. It is for all these reasons that we suggest that the UK's approach can validly serve as a pathfinder for countries looking to develop their public sector clouds but without wishing to reinvent this particular wheel.

Richard Kemp,
Kemp IT Law, London
October 2015
richard.kemp@kempitlaw.com

ANNEX - UK GOVERNMENT: SECURITY POLICY, DATA CLASSIFICATION, CLOUD SECURITY POLICY AND CLOUD MARKETPLACE GUIDANCE DOCUMENTATION[27]

No.	Title	Date	URL	Status (08.2015)
1.	**ICT STRATEGY**			
1.1	Government ICT Strategy[28]	March 2011	http://webarchive.nationalarchives.gov.uk/+/https://www.gov.uk/government/publications/uk-government-ict-strategy-resources	Superseded by 1.4[3]
1.2	Government ICT Strategy: Strategic Implementation Plan[3]	October 2011	https://www.gov.uk/government/publications/government-ict-strategy-strategic-implementation-plan	Superseded by 1.4[3]
1.3	Government Cloud Strategy	March 2011	https://www.gov.uk/government/publications/government-cloud-strategy	Not superseded
1.4	Government Service Design Manual	June 2015	https://www.gov.uk/service-manual	In effect
1.5	Digital by Default Service Standard	June 2015	https://www.gov.uk/service-manual/digital-by-default	In effect
2.	**SECURITY POLICY**			
2.1	Government Security Policy Framework	April 2014	https://www.gov.uk/government/publications/security-policy-framework	In effect
3.	**SECURITY AND DATA CLASSIFICATION**			
3.1	Government Security Classifications	April 2014	https://www.gov.uk/government/publications/government-security-classifications	In effect
3.2	Government Security Classifications Supplier Briefing	October 2013	https://www.gov.uk/government/publications/government-security-classifications	Current
3.3	Government Security Classifications – Supplier Slides	October 2013	https://www.gov.uk/government/publications/government-security-classifications	Current
3.4	FAQ 1 - Working With Official Information	April 2013	https://www.gov.uk/government/publications/government-security-classifications	Current
3.5	FAQ 2 – Managing Information Risk at OFFICIAL	March 2014	https://www.gov.uk/government/publications/government-security-classifications	Current

[27] The UK Government documents listed here are Crown Copyright and (mainly) licensed under the terms of the Open Government Licence (available at https://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/). The licence permits worldwide use and copying, publication, distribution, transmission and adaptation of content and commercial and non-commercial exploitation subject to acknowledgement and a default attribution of 'Contains public sector information licensed under the Open Government Licence v3.0'.

[28] Withdrawn July 2014, replaced by Service Design Manual

No.	Title	Date	URL	Status (08.2015)
4.	**CLOUD SECURITY**			
4.1	Overview - Summary of Cloud Security Principles	August 2014	https://www.gov.uk/government/publications/cloud-service-security-principles	In effect
4.2	Overview - Cloud Security Guidance: Introduction	August 2014	https://www.gov.uk/government/publications/cloud-security-guidance-introduction	In effect
4.3	Cloud Security Guidance: Risk Management	August 2014	https://www.gov.uk/government/publications/cloud-security-guidance-risk-management	In effect
4.4	Implementing the Cloud Security Principles	August 2014	https://www.gov.uk/government/publications/implementing-the-cloud-security-principles	In effect
4.5	Cloud Security Guidance: Separation	August 2014	https://www.gov.uk/government/publications/cloud-security-guidance-separation	In effect
4.6	Cloud Security Guidance: IaaS Consumer Guide	August 2014	https://www.gov.uk/government/publications/cloud-security-guidance-iaas-consumer-guide	In effect
4.7	Cloud Security Guidance: Standards and Definitions	August 2014	https://www.gov.uk/government/publications/cloud-security-guidance-standards-and-definitions	In effect
5.	**DIGITAL MARKETPLACE GUIDANCE**			
5.1	Digital Marketplace buyer's guide	Updated May 2015	https://www.digitalmarketplace.service.gov.uk/buyers-guide	In effect
5.2.1	G-Cloud Framework		https://www.digitalmarketplace.service.gov.uk/g-cloud/framework	G-Cloud 6 in effect
5.2.2	G-Cloud buyers' guide	Updated Sept 2014	https://www.digitalmarketplace.service.gov.uk/g-cloud/buyers-guide	Current
5.2.3	G-Cloud suppliers' guide	Updated Sept 2014	https://www.digitalmarketplace.service.gov.uk/g-cloud/suppliers-guide	Current
5.2.4	G-Cloud Service Definitions	November 2013	https://www.gov.uk/government/publications/g-cloud-service-definitions	In effect
5.3.1	Digital Services Framework		https://www.digitalmarketplace.service.gov.uk/digital-services/framework	In effect
5.3.2	Digital Service Store buyers' guide	November 2013	https://www.gov.uk/government/publications/digital-services-store-buyers-guide/digital-services-store-buyers-guide	Current
5.4	Crown Hosting Data Centres Framework		https://www.digitalmarketplace.service.gov.uk/crown-hosting/framework	In effect