Seeding the Global Public Sector Cloud: Part I - A Role for International Standards[1]

Abstract: This is the first of a two part paper that assesses current trends in the adoption of public sector cloud computing by governments around the world. It suggests a role for ISO standards, particularly ISO 27001 and ISO27018, in addressing security and risk management concerns as the biggest inhibitors to global public sector cloud uptake. 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.

All of a sudden, everywhere you look, the cloud is the new normal. Quarterly results published in July 2015 from Microsoft and Amazon, two of the top four cloud service providers, show cloud service revenues at each company almost doubling year on year to account for nearly ten percent of total revenues.[2] And this growth is just the start: research firm IDC predicts that spending on public cloud computing services will grow by twenty-three percent on average each year from 2014 ($57bn) to 2018 ($128bn), with Software as a Service (**SaaS**) growing from $40bn to $83bn and Platform (**PaaS**) and Infrastructure (**IaaS**) as a Service together growing from $16bn to $45bn.[3]

Up to now, the private sector has led the charge, with governments bringing up the rear. Even in countries with the most developed public sector cloud computing strategies, spend on cloud services has yet to reach five percent of central governments' IT budgets. In the USA, the Government Accountability Office recorded in September 2014 that spending on cloud services for seven US government departments had grown from $307m to $529m between 2012 and 2014 but still accounted for just 2 percent of their IT budgets,[4] although US federal government cloud spending is currently estimated at around $3bn in total, or roughly four percent of the total $80bn federal IT budget.[5] In the UK, spending on G-Cloud, the Government cloud services procurement initiative, in the 12 months to August 2015 was

---

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

[2] Q2 2015 net sales of Amazon Web Services (AWS) were $1.824bn, up 81% year on year and 7.9% of total Q2 revenues of $23.2bn (available at http://phx.corporate-ir.net/phoenix.zhtml?c=97664&p=irol-reportsother). For Microsoft, Q4 2015 commercial cloud revenue grew 88% to an annualised run rate of over $8bn, where $8bn would represent 8.5% of total FY 2015 revenues of $93.6bn (available at https://www.microsoft.com/investor/EarningsAndFinancials/Earnings/PressReleaseAndWebcast/FY15/Q4/default.aspx)

[3] IDC Press Release, *IDC Forecasts Public IT Cloud Services Spending Will Reach $127bn in 2018 as the Market Enters a Critical Innovation Stage* (3 November 2014) available at http://www.idc.com/getdoc.jsp?containerId=prUS25219014

[4] US Government Accountability Office, Highlights of Report to Congressional Requesters, *Cloud Computing: additional opportunities and savings need to be pursued* (September 2014) available at www.gao.gov/assets/670/666133.pdf. The seven departments were Agriculture, General Services Administration, Health and Human Services, Homeland Security, Small Business Administration, State and Treasury

[5] 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

£463m,[6] or roughly four percent of a total UK estimated Government ICT (information and communications technology) spend of £11bn or so. Industry forecasts however are for the public sector cloud to account for more than half global software and storage spending growth by 2018 and for US federal spending on cloud to reach $6.5bn by 2019, an annual average growth rate of twenty-one percent from today.[7]

Part I of this paper examines why government cloud computing development has been relatively slow to date and explores how inhibitors to uptake could be removed so as to facilitate the projected step change in public sector cloud growth. It suggests that security and privacy concerns, coupled with a particular approach in the public sector to risk management, are the main factors behind the slow adoption of the public sector cloud; and that these issues can effectively be addressed through a structured approach:

- developed from the centre and applied consistently across government;
- based on a robust classification of the different data types making up government work;
- effectively transposing that data classification to the cloud;
- setting substantive cloud security requirements for these different classes of data; and
- putting in place practical and effective procedures to manage cloud security based on authorisation, certification and audit techniques adopted by international standards, particularly ISO 27001 and ISO 27018.

Part II of the paper then considers how governments who have up to now stayed away from the 'bleeding edge' of the public sector cloud may re-use the benefits of work already done elsewhere in this area and without having to reinvent the wheel, and will suggest the UK's structured approach and published framework as a potential pathfinder.

Understanding the Cloud: Terminology, Benefits and Blockers

Briefly, the classic NIST definition[8] of the cloud specifies a type of computing with five key characteristics, three service models and four deployment models. The characteristics are *on demand self-service*, *network access*, *one-to-many provisioning* (resource pooling or demand diversification), *rapid scaling* (elasticity) and measure *(metered) service*; the elements of the *SaaS*, *PaaS* and *IaaS* service models are shown at 1, 2 and 3 in Figure 1 below; and the four deployment models are *private cloud* (where infrastructure, platform and/or software are used solely for a single cloud service customer), *community cloud* (solely for use by a community of customers, rather than a single customer) *public cloud* (where service is provided on the cloud service provider's premises to their customers on a multi-tenant basis) and *hybrid cloud* (private cloud with access to public cloud to manage peaks and load balancing).

Within this general framework many countries have articulated what they mean by cloud services. For example, at EU level ENISA (the European Union Agency for Network and Information Security) has characterised 'Gov Cloud' as a deployment model that:

[6] available at http://govspend.org.uk/g-cloud.php

[7] Sources: *IDC Worldwide and Regional Public Cloud IT Services 2014 – 2018 Forecast* and *Deltek Federal Industry Analysis* cited in the Forbes Insights Report at footnote 5 above

[8] available at http://www.nist.gov/itl/cloud/

"builds and delivers services to state agencies (internal delivery), citizens and enterprises (external delivery) [*the who*] in an environment where services are compliant with security, privacy and resilience laws [*the what*] under public body governance in a secure and trustworthy way [*the how*]".[9]

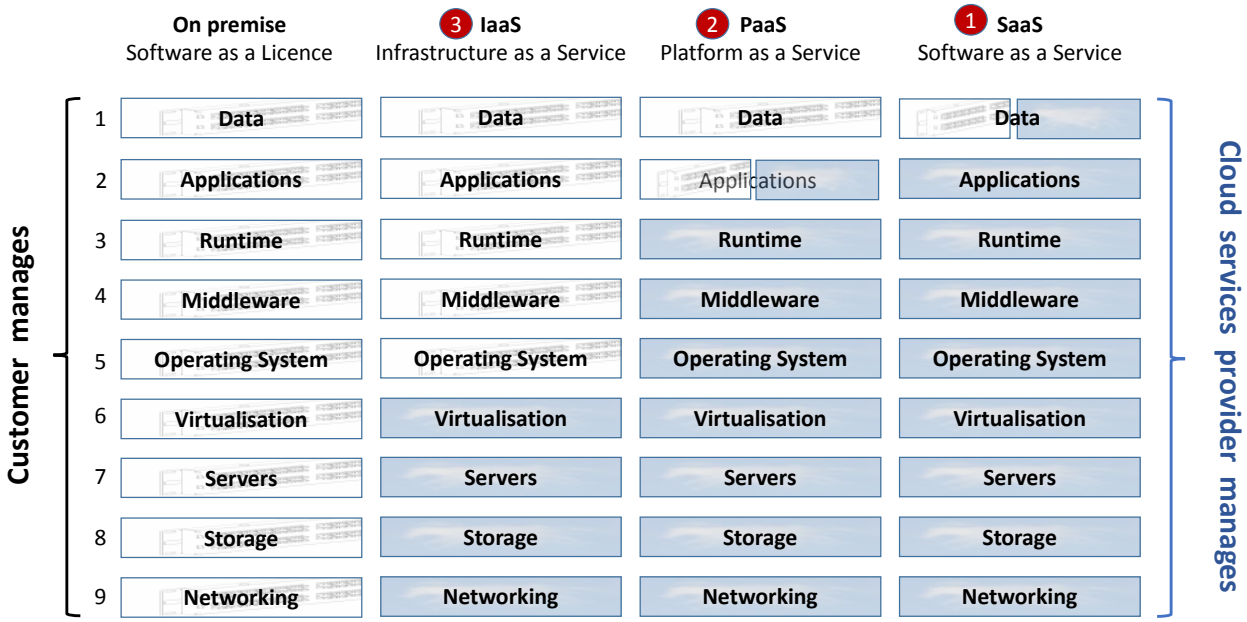
The UK government describes cloud computing as follows:

"instead of hosting applications and data on an individual computer, everything is hosted in the 'cloud' – a collection of servers accessed via the internet or private network"

and crisply articulates the benefits:

"by exploiting cloud computing, we will transform the public sector ICT estate into one that is agile, cost effective and environmentally sustainable".[10]

Figure 1: Software as a Licence to Software as a Service: the Cloud Service Model Continuum



The benefits were set out in broadly similar terms in the US Federal Cloud Computing Strategy:

"cloud computing has the potential to play a major part in … improving government service delivery and … significantly help[ing] agencies grappling with the need to provide highly reliable, innovative services quickly despite resource constraints".[11]

[9] ENISA *Security Framework for Governmental Clouds* (26 February 2015) available at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/governmental-cloud-security/security-framework-for-govenmental-clouds

[10] UK Government Cloud Strategy, (March 2011) available at https://www.gov.uk/government/publications/government-cloud-strategy

[11] US CIO (8 February 2011) available at www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf

Economics of the Cloud

The benefits are real and evidenced, particularly in terms of the cost savings between private and public cloud:

> "For large agencies with an installed base of approximately 1,000 servers, private clouds are feasible but come with a significant cost premium of about 10 times the cost of a public cloud for the same unit of service, due to the combined effect of scale, demand diversification and multi-tenancy".[12]

Competitive trends, particularly among Amazon, Microsoft and Google as the providers with the deepest pockets, are driving even larger, hyper-scale, clouds - think $1bn+ investments, 1m+ square foot data centres with 100,000+ servers using enough energy to power a city. The cost benefits become even greater at this scale, but they are not the only thing. According to Accenture, every organisation will see "the benefits of 'hyperscale' innovation trickle into their data centers in the form of cost reductions" and other enablers for the organisation's development.[13]

But equally real are the reasons behind the slow adoption of public sector cloud computing up to now. In its February 2015 paper on *Security Framework for Governmental Clouds*[14], ENISA concluded that:

"
- The state of deployment of Governmental Cloud computing is in general at a very early stage …
- *Security and privacy issues* are considered as key factors to take into account for migration and at the same time *are the main barriers for adoption* …
- The main security challenges, requirements and barriers in the cloudification of governmental services are related to: *data protection and compliance*, interoperability and data portability, identity and access management, *auditing,* adaptability and availability, as well as *risk management* and detailed security SLA formalization.
- *… there are no guidelines to define a generic security framework that allows to assess and benchmark Gov Cloud security* (emphasis added)".

In similar, but more colourful, vein Big 4 accounting firm KPMG in a 2012 survey report of 430 public sector government executives from 10 countries[15] drew attention to a combination unique to public sector security concerns – the biggest worry - and approaches to risk:

> "*Concern with security was cited* by almost half of all government respondents (47 percent) *as their most significant concern* … Among the largest government entity respondents … the figure rises to 56 percent, the highest level of concern cited by any group. *However, almost 80 percent said they would be more confident if cloud services were certified by a government body* (page 4)".
>
> "*Government enterprises have less incentive to take on the risks of new and arguably untested technologies* [than the private sector]. 'In the public sector, if you take a risk and succeed, you may get a pat on the back but not much more; but if you fail – if your

[12] Microsoft Corporation, *The Economics of the Cloud* (November 2010), page 16 available at https://www.microsoft.com/en-gb/search/result.aspx?q=economics+of+the+cloud&form=apps

[13] Accenture, *Digital Business Era: Stretch Your Boundaries*, http://techtrends.accenture.com/us-en/business-technology-trends-report.html

[14] Footnote 9 above, at pages 7 and 8

[15] KPMG International, *Exploring the Cloud: A Global Study of Governments' Adoption of Cloud* (March 2012) available at http://www.forbes.com/forbesinsights/government_cloud_2012/index.html

> pensioners don't get their checks, or if you botch privacy protection – you will be in a world of trouble' (page 18) (emphasis added)".

A more recent survey in the UK public sector from July 2015 found that ninety-two percent of respondents cited data security when asked about barriers to confidence in and adoption of cloud computing.[16] Concerns are also highlighted about the dangers of dependency when governments transition to outside providers:

> "What if the outside providers don't handle security or privacy in ways the public expects and demands?"[17]

It is easy also to forget that governments play many highly visible roles in their in-country IT and cloud arenas, each of which provides a context for this nuanced approach to risk: they are the biggest buyer and user of ICT services in their country; increasing citizen interaction means government IT is highly visible when it goes wrong (never, one might add, when it goes right); as legislature, governments set policy, laws and norms on IT use; as executive, they carry out national policy for IT, including digital and cloud-first strategies and innovation in IT generally; and in many countries, cloud is at the forefront of a transformation of government services driven in part by the need to balance the books following the 2008 global financial crisis.

Against this background, what these papers, surveys and comments show is that risk management is at the centre of practical, front line, public sector worries about cloud adoption, and that removing them will be indispensable to unlocking potential for growth. When the risk/reward balance is characterised by 'a world of trouble' versus 'a pat on the back', public sector executives need to be able to breathe easily and remove the risk of trouble through effectively calibrated cloud security risk management. This explains why ENISA in February this year highlights the lack of a general cloud security framework to support benchmarking, auditing and risk management, why ninety-two percent of the 2015 UK public sector survey respondents cited data security as a barrier to cloud adoption and why eighty percent of the 2012 KPMG survey respondents advocated cloud certification. In short, not only must risk management be done; it must be seen to be done.

The Role of Government Policy in Cloud Adoption

Demonstrating effective management of cloud security risk is therefore a key *output* of a model security framework for public sector cloud computing. In order to achieve this, a number of other elements of the model need to be in place as *inputs*.

First, in order to ensure transparency, governments will be best placed when acting from the centre in establishing and publishing a cloud security framework and then using and applying this across all departments. This will ensure a consistency of approach that avoids the major risk of fragmentation that would otherwise arise with bespoke requirements and implementations.

---

[16] Chris Burt in Web Hosting Industry Review (WHIR) *Despite UK's Cloud First Policy, 36% of Government Workers Haven't Used Cloud Services* (7 July 2015) at http://www.thewhir.com/web-hosting-news/despite-uks-cloud-first-policy-36-of-government-workers-havent-used-cloud-services

[17] J. Mechling in Governing, *Government's Slow Takeoff into the Cloud* (5 March 2015) at http://www.governing.com/columns/smart-mgmt/col-government-slow-adoption-cloud-computing-collaboration.html

Second, they should adopt a robust classification of the different types of data that constitute their workloads, to reflect the fact that various government information assets are of different sensitivity and should thus be subject to differing handling guidelines.

Third, that data classification should be transposed effectively to the cloud. As will be shown in Part II of this paper in relation to the UK, effective data classification shows that up to 90% of a government's workload is, in principle and subject to appropriate controls, suitable for the public cloud. Data classification also puts in place a mechanism to identify those data assets which should always be held on premises and not leave the building.

Fourth, substantive baseline cloud security requirements should be mapped to the published data classification, so that each category of data is appropriately protected.

These four substantive elements – operating from the centre consistently across government, adopting a robust data classification, transposing it effectively to the cloud, and mapping baseline cloud security requirements to the data classification – support the critical procedural side of demonstrating good practice in managing cloud security risk.

The UK's approach[18] mandates baseline security controls reflecting good commercial practice for its 'business as usual' (in UK parlance, 'OFFICIAL') work, described as:

> "up to 90% of Public Sector business, including most policy development, service delivery, legal advice, personal data, contracts, statistics, case files, and administrative data".[19]

It states that security controls at this level: "are based on good, commercially available products in the same way that the best-run businesses manage their sensitive information"[20] where "information must be secured against a threat model that is broadly similar to that faced by a large UK company"[21] and "technical controls … will be based on assured, commercially available products and services".[22]

These statements are ground-breaking and more profound than would first appear. It is hard to overstate their impact. They signal a definite and intended change in approach to data classification by the UK Government, especially when one considers the extent of its definition of OFFICIAL information, as including "the day to day business of government, service delivery and public finance".[23]

Whilst many inside and outside government might come to the discussion with different preconceptions, the new approach is set against over-classification and turns on its head in a refreshingly open way the myth that somehow even the 'normal business of government' is highly sensitive.

The UK also states that off-shoring OFFICIAL information is permitted in principle, subject to the considerations one would expect – personal data should be kept within the EEA or

---

[18] UK Cabinet Office, *UK Government Security Classifications* (April 2014) available at https://www.gov.uk/government/publications/government-security-classifications

[19] UK Cabinet Office, *Introducing the Government Security Classifications – Core briefing for 3rd Party Suppliers* (October 2013) available at https://www.gov.uk/government/publications/government-security-classifications

[20] *Ibid*., page 2

[21] *UK Government Security Classifications*, footnote 18 above, Annex, paragraph 1, page 17

[22] *UK Government Security Classifications*, footnote 18 above, Annex, paragraph 4, page 17

[23] *UK Government Security Classifications*, footnote 18 above, page 7.

elsewhere as permitted by data protection law; off-shoring may not be suitable for data relating to national security; and the destination environment must be consistent with meeting applicable cloud security requirements.[24] This again is a pragmatic approach that allows the cost benefits of the cloud to be harnessed by the public sector: data localisation in-country is possible of course, but likely at a higher cost.

A Growing Role for International Standards

An intrinsic part of this approach to demonstrating cloud security management by reference to good commercial practice is the use of international standards. The UK's Cloud Security Guidance on Standards[25] references ISO 27001 as a standard to assess implementation of one or more Cloud Security Principles, and ISO 27001 certification is generally expected for approved providers of UK G-Cloud services. Just as the UK's approach may help other countries as a pathfinder to their own model cloud security framework, so ISO 27001 procedures and certifications can provide confidence around the world to countries looking to implement the critical procedural side of demonstrating good practice in managing cloud security risk.

The International Organisation for Standardisation (**ISO**), based in Geneva, Switzerland, is the world's largest developer of voluntary international standards.[26] Established in 1946, it operates as a network of the 162 national standards bodies who are its members. For example, the UK's member is BSI (the British Standards Institution), Germany's is DIN (Deutsches Insititut fur Normung e.V.) and the USA's is ANSI (the American National Standards Institute), each of whom while not stated owned, is recognised by their country as the sole organisation for issuing standards having a national application.[27] Technical standards work is undertaken by one of three hundred or so technical committees. In active standards areas like the Cloud, ISO keeps close links with other standards setting organisations (**SSO**s) and international bodies active in the field.

ISO publishes many 'families' of related standards, of which the best known is the ISO 9000 family on quality management systems, first published in 1987. The ISO 27000 series is a growing family of forty or so standards on '*Information Technology – Security Techniques – Information Security Management Systems*' (**ISMS**). ISO 27001[28] sets out formal ISMS

---

[24] *FAQ 2 – Managing Information Risk at OFFICIAL,* March 2014, page 9, available at https://www.gov.uk/government/publications/government-security-classifications

[25] By CESG (the Communications-Electronic Security Group, part of GCHQ (the UK Government Communications Headquarters) *Cloud Security Guidance: Standards and Definitions* (14 August 2014) available at https://www.gov.uk/government/publications/cloud-security-guidance-standards-and-definitions

[26] http://www.iso.org/iso/home.htm

[27] BSI was established as the Engineering Standards Committee of the British Iron Trade Association in 1901; incorporated by Royal Charter in 1929; changed its name to BSI in 1931; and was officially recognised as the only UK standards issuer in 1942. The DIN was established in 1917 by the Verein Deutscher Ingenieure (VDI – Society of German Engineers); converted to the Deutscher Normenasschuss (DNA – General Committee for Standardisation) in 1926; and changed its name to DIN and signed a Standards Treaty with the federal government in 1975. ANSI was established as the American Engineering Standards Committee (AESC) in 1916; was reorganised as the American Standards Association (ASA) in 1928; affiliated with the US National Committee of the IEC (International Electrotechnical Commission) in 1931; was reorganised at the USASI (United States of America Standards Institute) in 1968; and adopted its present name in 1969

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

control objectives and controls against which an organisation can be certified, audited and benchmarked. Organisations can request third party certification assurance and this certification can then be provided to the organisation's customers.[29]

ISO conducts an annual survey on the global uptake of ISO 27001 certificates[30], which grew by 22.1 percent from 19,620 in 2012 to 23,972 in 2014. ISO 27001 certificate growth in a number of selected Eastern European EU Member States and African, Middle East and Asian countries is shown in Figure 2 below for the years 2011 to 2014. The totals for the six EU Member States shown in the table represents approximately ten percent of the worldwide total for each of 2012, 2013 and 2014.

Figure 2: Evolution of ISO 27001 Certificates between 2011 and 2014 in Selected Eastern European EU, African and Middle East and Asian Countries

Country/Group	2011	2012	2013	2014
A. Eastern Europe EU				
Bulgaria	132	208	278	330
Czech Republic	301	264	397	276
Hungary	178	199	280	297
Poland	233	279	307	310
Romania	575	866	840	893
Slovakia	111	127	119	162
TOTAL	**1,530**	**1,943**	**2,221**	**2,268**
B. Africa				
Egypt	6	11	17	11
Nigeria	5	9	12	16
South Africa	14	22	35	22
TOTAL	**25**	**42**	**64**	49
C. Middle East				
Qatar	9	7	23	28
Saudi Arabia	37	46	59	72
UAE	73	96	123	131
TOTAL	**119**	**149**	**205**	**231**
D. Asia				
Indonesia	29	35	48	64
Korea	191	230	252	288
Malaysia	72	100	181	233
Philippines	59	66	73	47
TOTAL	**351**	**431**	**554**	**632**
GRAND TOTAL	**2,025**	**2,565**	**3,044**	**3,180**

[29] See EY Insights on governance, risk and compliance, *Building trust in the cloud: Creating confidence in your cloud ecosystem* (June 2014) available at http://www.ey.com/GL/en/Services/Advisory/Building-trust-in-the-cloud

[30] ISO's annual survey of the world distribution and evolution of ISO/IEC 27001 certificates is at http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certificate=ISO/IEC%2027001

One of the most recent additions to the ISO 27000 family is ISO 27018[31] as a '*Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*'[32]. ISO 27018 extends the requirements of ISO 27002[33] (the underlying generic code of practice on controls regarding the confidentiality, integrity and availability of information systems) in ways that are appropriate and specific for public cloud service providers handling PII (PII is effectively the same thing as personal data in the EU).

Examples of entirely new controls suggested by ISO 27018 include requirements for the cloud service provider as the organisation processing PII:

- that media leaving the organisation's premises are subject to an authorisation procedure and (e.g. through encryption) is not accessible to unauthorised personnel (Annex A.10.4);
- to maintain a current record of all users with authorised access to systems and a current user profile for all users with authorised access to PII (Annex A.10.9); and
- to ensure for all data storage space assigned to a cloud service customer that any data previously residing on that space is not visible to that customer (Annex A.10.13).

Public sector authorities are therefore able to leverage the augmented security and privacy controls that ISO 27018 introduces as the security baseline for the core of their public sector 'business as usual' data, which will often contain PII or other sensitive but non-national security related information ('OFFICIAL' in the UK's data classification).

A recent example of public sector take up of ISO 27018 is the draft policy published in the Philippines providing that Government departments using cloud computing are mandated to follow ISO 27002 and ISO 27018 to protect the confidentiality, integrity and availability of data.[34] The February 2015 ENISA *Security Framework for Governmental Clouds* report also refers at Annex A to compliance with ISO 27002 (and ISO 27001) as an appropriate security standard in responding to questions seeking to assess and evaluate security dimensions around confidentiality, integrity and availability.[35]

In a world where authorities are sceptical (appropriately so in some cases) about cloud service providers' self-asserted statements and even contractual commitments about how their data is stored, accessed and used in-cloud, proof of adherence to ISO standards and successful third party audits by an independent third party adds a worthwhile level of assurance. Authorities who plan to rely on independent third party ISO certification will want

---

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

[32] See, *What you need to know about the growing role of ISO data and security standards in cloud contracts,* Kemp, Cloud Computing Intelligence (24 October 2014) available at http://cloudcomputingintelligence.com/features/item/1600-what-you-need-to-know-about-the-growing-role-of-iso-data-and-security-standards-in-cloud-contracts

[33] http://www.iso27001security.com/html/27002.html

[34] The Republic of the Philippines Department of Science and Technology draft policy on '*Adopting Cloud Computing as an ICT Deployment Strategy for Delivering Services in the Government*' (available at http://icto.dost.gov.ph/draft-policies/). The draft policy, which was the subject of a Public Hearing at Diliman, Quezon City on August 20, 2015, provides at Section 8 (Information Security Compliance) that "Government Institutions, in adopting cloud computing, shall protect the confidentiality, integrity and availability of data. The use of ISO/IEC 27002:2013 as augmented by ISO/IEC 27018:2014 is hereby mandated as the minimum requirement in preparing the information security management system."

[35] Annex A and B, page 24 available at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/governmental-cloud-security/security-framework-for-govenmental-clouds. See also footnote 9 above.

to see more than just the certificate itself. They will also want to carefully review all relevant documentation relating to the scope of the audit and the long form audit report issued by the certification body, which it is understood that a number of cloud service providers are willing to provide subject to appropriate confidentiality arrangements.

Other factors for authorities to take into account in reviewing standards and audits include the elapsed time since the cloud services provider had its last comprehensive audit (certifications may operate on a three year audit cycle for example) and its last interim check-up (which may take place annually). This becomes particularly important where a prospective provider has opened or acquired a new data centre since the last audit or check-up that the authority is proposing to use. In this case the authority will need to satisfy itself that the evidenced standard or audit applies to the place where its work will be processed.

In addition to timing aspects of standards and audits, authorities may also need to consider the issue of international certification equivalence – the ability to recognise (or not) in their own country a standard or audit certification presented to them by a cloud service provider but obtained in a different geography. An authority proposing to contract in its own country (A) with a provider presenting a certificate obtained in another country (B) will need to satisfy itself that the rigour and reliability of the standards auditor and auditing requirements in country B demonstrate sufficient assurance of compliance in the authority's own country A. As cloud standards become more widespread, international equivalence and recognition regimes for standards certification – perhaps looking a bit like the national treatment principle under international intellectual property conventions – look set to develop and become more important.

ISO 27001 and ISO 27018 provide a method that is widely globally used, increasingly popular internationally and comes with the ISO's hallmark of quality and reassurance for public sector executives around the world to address concerns about cloud security through demonstrable and demonstrated procedures designed to assess, certify, benchmark and audit achievement of cloud security standards. Authorities naturally should be diligent for the contracts they let to ensure that the standards a prospective provider presents them with are fit for purpose. Operated in this way, ISO 27001 and ISO 27018 provide a particularly useful tool to helping unlock growth in public sector cloud uptake around the world.

Conclusions

This paper has sought to show how security and privacy concerns, as the main blockers to public sector cloud uptake, can effectively be addressed through a structured approach developed from the centre and applied consistently across government. This approach places appropriate weight on substantive requirements as inputs and on demonstrated procedures as outputs. Substantive inputs start with a robust classification of the different types of data that make up governments' workloads – where the UK's April 2014 security reclassification is truly ground-breaking and profound. This is then transposed to the cloud, enabling substantive cloud security requirements to be set for those different classes of data. Effective, evidenced procedures to manage cloud security risk can be then based on authorisation, certification and audit techniques adopted by international standards, particularly ISO 27001 and most recently ISO 27018.

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