Scotland's Digital Future: Scottish Public Sector Cloud Computing Guidance

Digital Scotland

The Scottish Government
Riaghaltas na h-Alba

Contents

Introduction

Scotland's Digital Future: Delivery of Public Services set out an objective of developing a national strategy for the public sector's data storage focusing on consolidation and re-use. This reflected a recommendation of the Review of ICT Infrastructure in the Public Sector in Scotland report by John McClelland which suggested that significant efficiency and energy savings could be achieved through consolidation.

The strategy Scotland's Digital Future: Data Hosting and Data Centre Strategy for the Scottish Public Sector for the Scottish Public Sector sets out how we will deliver on that overall objective and in particular how the public sector will adopt the following approaches for achieving significant efficiency and energy savings: cloud computing, virtualisation and co-location.

This document delivers on the priority action within the strategy to set out the cloud policy for the public sector, and provide the guidance and principles for how Scotland's Public Sector will use the cloud. In assessing the current approach and environments we found that organisations face many options in making arrangements for data hosting but lack both an overall vision and information base for doing so, and need guidance on how best the Scottish public sector use cloud computing.

The decision roadmap in the data hosting and data centre strategy sets out what organisations should consider in terms of new investment or change to the delivery or hosting of services.

Cloud computing is a priority option in the overall strategy and organisations must consider how they can adopt the policy and deliver the efficiency and flexibility that this can offer. Cloud computing is an evolving and broad topic on which almost everyone has a perspective and an opinion. Our overall policy position is that cloud computing is part of the strategic future of digital public services in Scotland. It has potential to fundamentally change the nature of digital public service delivery and, when appropriately utilised, can provide benefits in cost effectiveness, energy efficiency and speed of deployment.

Cloud computing is a new approach to the delivery of ICT services in Scotland's Public sector that can deliver:

- "anywhere" access to shared computing resources
- "freedom" from capital expenditure on back-end computing equipment and software
- the ability to provision computing services very quickly and cheaper than traditional models, and
- the ability to pay for such services on some form of metered or per-use basis

Delivering on the overall policy position will mean –

- cloud computing is the dominant solution of our Digital Public Services delivery
- we reduce the number of data centres in line with the strategy Scotland's Digital Future: Data Hosting and Data Centre Strategy for the Scottish Public Sector
- we deliver multi-vendor procurement frameworks to ensure external service providers have the opportunity to fulfil our requirements and in doing so maximise competition
- we investigate with public sector partners the opportunities to create a Scottish public sector community cloud

Who is the policy aimed at?

In line with the approach of and commitments in "Scotland's Digital Future: Delivery of Public Services", this policy has been developed with and for the Scottish public sector and their partners to maximise the benefits of an aggregated approach to delivery. The sectors in scope are:

- Central Government including Police and Fire
- Local Authorities
- Health
- Further and higher education

The policy will also be available to the third sector and in particular is appropriate where they are supporting the direct delivery of public services.

Principles

- cloud based solutions will be the dominant approach for the Scottish public sector
- the assessment criteria and guidance on the procurement and usage of cloud offerings that is being developed will be adopted
- utility and cloud computing is considered in assessing the appropriateness of current arrangements and future investment plans, and a shift to the cloud takes place when this is the most cost-effective option that delivers business requirements

The principles and approaches will be aligned to the development of the European Commission's European Cloud Computing Strategy[1] and will be kept under review and amended or supplemented as cloud computing and legislation evolves and lessons are learned from the adoption and accelerated growth within the public sector.

[1] http://ec.europa.eu/information_society/activities/cloudcomputing/index_en.htm.

Definitions

There is a lot of confusion and misunderstanding of what cloud computing means to individuals and organisations. To enable greater understanding and consistency in the language used, the Scottish public sector will adopt the US Government's National Institute of Standards and Technology (NIST) definition of Cloud Computing.

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models."

Five Essential Characteristics	Three Service Models	Four Deployment Models
• On-demand self-service • Broad network access • Resource pooling • Rapid elasticity • Measured service	• Software as a Service (SaaS) • Platform as a Service (PaaS • Infrastructure as a Service (IaaS).	• Private cloud • Community cloud • Public cloud • Hybrid cloud

The definitions, described in more detail in Annex 1, are intended to help those developing policy or the adoption of solutions in cloud computing to develop a consistent framework of understanding, with common frames of reference and simple taxonomies. These definitions are not intended to prescribe or constrain any particular method of deployment, service delivery, or business operation.

Benefits

Cloud computing offers numerous advantages both to end users and organisations of all sizes. One of the biggest advantages is that you would no longer have to support some or all of your ICT infrastructure. As this responsibility is reduced it allows organisations to focus on their core business. Some of the other benefits include:

- **Cost:** This is the biggest headline advantage of cloud computing and is achieved by the reduction in investment in stand-alone software or servers. By leveraging the scalability and flexibility available through cloud computing, organisations can reduce overhead charges such as the cost of data storage, software updates, management etc. The majority of costs are now transferred from CapEx to OpEx and the service price includes all necessary hardware and software. Computing then becomes an operating expense rather than a capital expense. Cloud platforms provide direct visibility into your IT spending where you can see exactly what a cloud platform is charging you for. This greater transparency can help you make better decisions about the services you provide.

- **Increased storage capacity:** Cloud computing can accommodate and store much more data compared to a personal computer and in a way offers almost unlimited storage capacity. It eliminates worries about running out of storage space and at the same time it spares businesses the need to upgrade their computer hardware, further reducing the overall IT cost.

- **Scalability:** Cloud services enable an individual or organisation to access computer services on a pay-as-you-go basis, with the flexibility to scale up and down as needed for little marginal cost. Scalability is a built-in feature for cloud deployments. Cloud instances are deployed automatically only when needed and as a result, you pay only for the applications and data storage you need. They also provide elasticity, since clouds can be automatically scaled to meet your changing IT system demands.

- **Strong security:** Cloud service providers can offer organisations better security, reliability and access to the latest upgrades than would otherwise have been possible through traditional in-house solutions.

- **Energy efficiency:** Cloud computing has the potential to leverage modern technologies such as computer virtualisation so reducing carbon footprint due to the more efficient use of computer hardware that requires less electricity and less air conditioning. The cloud is in general more efficient than a traditional ICT infrastructure and it takes fewer resources to compute, thus saving energy. For example, when servers are not used the infrastructure normally scales down freeing up resources and consuming less power. At any moment, only the resources that are truly needed are consumed by the system.

- **Business continuity:** With the computing infrastructure typically located in multiple physical locations for improved disaster recovery the process of backing up and recovering data is simplified since it now resides on a cloud infrastructure

and not on restricted physical devices. In some cases, the cloud itself is used solely as a backup repository for an organisations data.

- **Core business focus:** To enable organisations to focus on their core business, support staff currently employed to maintain hardware can be redeployed in areas that can provide business benefits.

- **Capability:** This can provide organisations with the ability to do things quicker and without new investment in servers enabling immediate access to infrastructure.

- **Resiliency and redundancy:** A cloud deployment is usually built on a robust architecture thus providing appropriate resiliency and redundancy to its users. The cloud offers automatic failover between hardware platforms out of the box, while disaster recovery services are also often included.

Security Considerations

As made clear from the above, cloud computing is a tool that offers enormous benefits to its adopters. However, being a tool, it also comes with some challenges when deploying in a public sector environment. It is continually evolving and there is still uncertainty and challenges that organisations need to understand. Organisations need to balance the headline benefits while considering the appropriate balance of risk relating to security.

An organisation's assessment of the risk to their information or services should not differ when assessing it in the cloud to how they would if it was on-site. What does differ is some of the questions that need to be considered, but the impact will remain the same. As with any information security assessment there are a variety of risks that need to be carefully considered, with the level of risks varying depending on the sensitivity to the organisation of the data being stored or processed.

However, benefits can only be fully realised following an assessment of the relative benefits and risks of any individual cloud service offering. All ICT has risk associated with it. For example, data stored at home are susceptible to theft or hardware failure. Cloud computing is not inherently more or less risky than traditional ICT, but the relative risks are different.

- **Confidentiality:** Organisations should have full ownership of their data and may want to specify the physical location of data stored or where it should not be stored. Consideration should be given to the impact of local regulations in countries where their data may be stored e.g. The USA Patriot Act and Regulation of Investigatory Powers Act 2000. Organisations using cloud computing to store or process publicly available data, such as a public web site may not be concerned about confidentiality. However, the organisation risk assessment should consider the availability and integrity of the public data, including reputational and other damage if the organisations system is offline, or is compromised and distributes misleading information or malicious content.

- **Integrity:** Data portability is a key mitigating strategy against vendor lock-in for cloud data storage services. Organisations should understand what is involved in moving from one vendor to another to allow them to continually get best value for their organisation

- **availability:** As organisations integrate more business capabilities with cloud computing there is a greater need for reliable internet connectivity. Downtime has the potential to have a negative impact on operations, similar to the loss of other services such as electricity or water. While the programme in Scotland to roll out Next Generation Broadband by 2020 will assist connectivity greatly, organisations should understand the implications of internet availability in their business continuity plans.

- **contractual:** When entering into a contractual arrangement there are a number of areas that should be understood, the key to getting the maximum benefit from the cloud is having the correct SLA for your service.

The assessment question list at Annex 2 should be considered when thinking about using cloud computing, this will assist in making an informed decision as to whether cloud computing is currently suitable to meet business goals with an acceptable level of risk.

It is recommended that any risk assessment is undertaken by digital business leaders as well as the ICT department in liaison with the information assets owner.

Updated guidance for organisations that need to assess and make business decisions about technology and information risks has been published by CESG see . https://www.gov.uk/government/publications/technology-and-information-risk-management

Any risk assessment should also consider a privacy impact assessment (PIA) see Annex 3.

Cloud Standards

Standards:

- CESG - Cloud Security Guidance
- Cloud Security Alliance (CSA)
- Common Assurance Maturity Model (CAMM)
- FedRAMP (U.S. Federal Government)

Guidelines:

- payment cards industry data security standards - https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf
- NIST cloud computing guidelines for managing security and privacy - http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909494
- EU European Cloud Strategy - https://ec.europa.eu/digital-agenda/node/10565

Certification Programs:

- ISO/IEC 27001,27002,27017

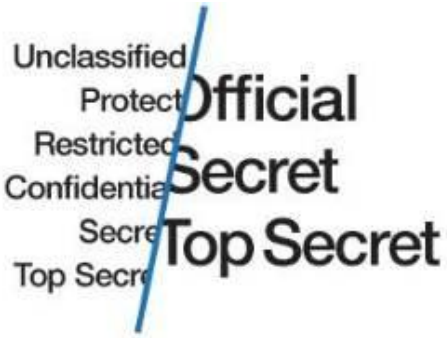
Information Classification

All information that the public sector in Scotland needs to collect, store, process, generate or share to deliver services and conduct public business has intrinsic value and requires an appropriate degree of protection.

Security considerations are of paramount importance when selecting a hosting provider. It is therefore essential that any solution is approved to the impact level of the service you want to host there.

The various different data sensitivity requirements for organisations hosting their data have always been classified using the Government Security Classification scheme and or with a Business Impact Level (BIL) which ranges from 0 (zero) to 6. Zero being the lowest if the data is compromised and has no impact on the organisation through to 6 which has critical impact.

On 2nd April 2014 the governments data classification scheme changed, the change saw the reduction from 6 existing classifications (unclassified, protect, restricted, confidential, secret, top secret) and the end of the BIL.



The new classification is

- **Official** - The majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.

- **Secret** - Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage military capabilities, international relations or the investigation of serious organised crime.

- **Top secret** - HMG's most sensitive information requiring the highest levels of protection from the most serious threats. For example, where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

Any solution for hosting data whether it's in the cloud or otherwise should be maintained to a standard that complies with the classification and impact level an organisation categorises their data or service at after an impact assessment.

For a full explanation of using a risk assessment to identify BIL's you can read them on the CESG website here

http://www.cesg.gov.uk/publications/Documents/is1_risk_assessment.pdf

Business Impact Level Assessment

There will however be a transition period but it is expected that hosting suppliers who deliver services using compliance at a particular BIL or IL level will continue to operate in that manner for the foreseeable future.

Therefore the existing Business Impact Level structure should continue to be used in the course of an information risk assessment process until new guidelines are published.

Further information on working with Government security classification and the use of impact levels can be found here

https://www.gov.uk/government/publications/government-security-classifications

Case studies

Service Model	Advantages	Disadvantages	Exemplar
Platform as a Service	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. Languages, libraries, services, and tools supported by the provider.		
	• reduced Capex costs for the following reasons: 1. with hosted managed services all hardware and some of the software is rented so the customer pays only for what they use (expenditure may also be more predictable) 2. in addition an added advantage of PaaS is that the provider manages all hardware, software patching and update, physical & software security and day to day routine operational tasks (so there is a reduction in the need for on-site specialist staff) Given this PaaS can offer lower Op Ex costs than hosted managed services	• potential of vendor lock in. • lack of control on workloads.	**Improvement Service** The Improvement Service (IS) recently looked at the options for renewing a number of their aged services that were currently delivered through multiple suppliers with individual contracts which was complex to manage. The technology stack and hardware was hosted in co-location facility. IS developed a cost model and business case to understand the cost-benefit of various options for upgrading and simplifying their services in scope ranging from reuse and virtualisation of the existing assets through to renewal based on a managed service wrapped around an open source platform. The solution is now hosted in a private cloud for less than half the price that IS were currently paying. This also included 24/7 telephone support for citizens and public sector service providers. No staff costs were included in this saving as it was agreed upfront that no staff losses would be incurred as part of the “outsourcing” of the service. The existing staff and operating model within the IS has been adapted with key roles to support the new managed service contract.

	• convenience and agility is a major advantage of both as neither entail local installation, so the implementation and scale-up speeds can be much quicker than other service types • security is often provided, including data security and backup and recovery • makes research and development possible for 'non-experts' • flexibility - customers can have control over the tools that are installed within their platforms and can create a platform that suits their specific requirements • adaptability - features can be changed if circumstances dictate that they should • teams in various locations can work together; as an internet connection and web browser are all that is required, developers spread across several locations can work together on the same application build		

<table>
<tr><td rowspan="2">Software as a Service</td><td colspan="3">The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.</td></tr>
<tr><td>no capex costs as SaaS is subscription based and can also include upgrades, maintenance and customer support depending upon subscription level
easily connected as a browser and an internet connection is all that is required
as software is already up and running on the vendor’s data centre, there is a lack of tasks associated with licensed software upgrades and deployment time tends to be much shorter
scalability as the client simply adjusts the monthly subscription fee, thus removing a significant workload from in-house IT department</td><td>lack of convenience as not everything can be delivered through SaaS
software integration can be problematic if the customer adopts multiple SaaS applications, or wishes to connect to existing on-premises applications</td><td><u>University of Dundee – Microsoft Office 365</u>

The University of Dundee is a leading university in the United Kingdom, internationally recognized for its expertise across a range of disciplines, including science, medicine, engineering, and art.
The university looked to replace its GroupWise Novell email system with a hosted solution to improve reliability and communications and lower IT costs.
The university selected Microsoft Office 365 because it gave them an opportunity to go beyond just email (Lync, SharePoint) and broaden the communication capabilities that it offers to students and staff.
The case for Office 365 was also about reducing the total cost of ownership of the university’s messaging solution. The university expects to reduce costs by £500,000 over five years, based on reduced IT administration and maintenance, lower infrastructure costs, and reduced staffing levels required to support the email system and its users.
For hardware, the ICS department no longer has to acquire new servers or support the 40 servers previously dedicated to the GroupWise email system.
The university has also avoided costs that would have been required had it decided to increase storage for the GroupWise email system</td></tr>
</table>

Infrastructure as a Service.	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g. host firewalls).		
	• dynamically choose a CPU, memory, and storage configuration to suit your needs • immediate access to unlimited computing power • eliminates the need for investment in rarely used IT hardware • IT overheads handled by the IaaS cloud computing platform vendor • in-house IT can be dedicated to an Organisations core services	• there is a security risk of unauthorised access to an organisations data using IaaS in the public cloud • IaaS cloud computing platform model is dependent on internet availability	

Annex 1 – Cloud Model Definitions

Five Essential Characteristics:

1. ***On-demand self-service****.* A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

2. ***Broad network access.*** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

3. ***Resource pooling.*** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data centre). Examples of resources include storage, processing, memory, and network bandwidth.

4. ***Rapid elasticity.*** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

5. ***Measured service.*** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Three Service Models:

1. ***Software as a Service (SaaS).*** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

2. ***Platform as a Service (PaaS).*** The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications

created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. languages, libraries, services, and tools supported by the provider.

3. ***Infrastructure as a Service (IaaS).*** The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Four Deployment Models:

1. ***Private cloud.*** The cloud infrastructure is provisioned for exclusive use by a single organisation comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organisation, a third party, or some combination of them, and it may exist on or off premises.

2. ***Community cloud.*** The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organisations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organisations in the community, a third party, or some combination of them, and it may exist on or off premises.

3. ***Public cloud.*** The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organisation, or some combination of them. It exists on the premises of the cloud provider.

4. ***Hybrid cloud*****.** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardised or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Annex 2 – Suggested risk assessment considerations and questions

Confidentiality
Can your cloud provider provide an appropriate third party security assessment? Does this comply with an appropriate industry code of practice or other quality standard?
How quickly will the cloud provider react if a security vulnerability is identified in their product?
Is all communication in transit encrypted? Is it appropriate to encrypt your data at rest? What key management is in place?
Will the cloud provider delete all of your data securely if you decide to withdraw from their cloud in the future? What are the data deletion and retention timescales? Does this include end-of-life destruction?
Find out if your data, or data about your cloud users will be shared with third parties or shared across other services the cloud provider may offer.
Integrity
What audit trails are in place so you can monitor who is accessing data?
Make sure that the cloud provider allows you to get a copy of your data, at your request, in a usable format.
How quickly could the cloud provider restore your data (without alteration) from a back-up if it suffered a major data loss?
Availability
Does the cloud provider have sufficient capacity to cope with a high demand from a small number of other cloud customers?
How could the actions of other cloud customers or their cloud users impact on your quality of service?
Can you guarantee that you will be able to access the data or services when you need them?
If there was a major outage at the cloud provider how would this impact on your business?
Contractual
Make sure you have a written contract in place with your cloud provider.
How will the cloud provider communicate changes to the cloud service which may impact on your agreement?
Require the cloud provider contractually to operate within defined jurisdictions. Which countries will your cloud provider process your data in and what information is available relating to the safeguards in place at these locations? Can you ensure the rights and freedoms of the data subjects are protected?
You should ask your cloud provider about the circumstances in which your data may be transferred to other locations including countries.
Can your cloud provider limit the transfer of your data to countries that you consider appropriate?
Ensure that you have locked in maximum pricing on renewal of cloud agreements.

Ensure that you are clear about what is included, and watch out for typically unrecognised costs such as storage and premium maintenance.
Know and update your switching/exit cost, ensuring that you can exit contracts and get your data out effectively and efficiently.
Seek contractual uptime and performance guarantees that meet your business needs, and beware of exclusions to those guarantees.
Require the cloud provider to inform you when law enforcement authorities request personal information in the cloud

When an organisation has an understanding of what the answers to these areas mean for them, it can decide on the next steps for ways to move to the cloud, although this might include different approaches for different types of cloud services such as:

- cloud computing infrastructure services to host enterprise applications
- cloud computing infrastructure services to build new applications
- creation of composite mashups (running internally or externally) to combine and leverage multiple cloud services
- cloud computing application and information services

Annex 3 - Privacy impact assessments (PIAs)

The information commissioner's office has published guidance on assessing the impact of moving information into the cloud.

They have published a Conducting privacy impact assessments code of practice which explains what PIAs are and how you can use them in your organisation.

The code contains annexes which can be used as the basis for your PIA. These include questions to guide the process and templates for recording the assessment. You do not have to use these if you would prefer to follow your own process, but the annexes are included in an editable format.

An assessment of the impact of the risk to sensitive and personal information should be undertaken prior to moving data into any location and particularly the cloud.

Privacy impact assessments (PIAs) are a tool that you can use to identify and reduce the privacy risks of your projects. A PIA can reduce the risks of harm to individuals through the misuse of their personal information. It can also help you to design more efficient and effective processes for handling personal data.

You can integrate the core principles of the PIA process with your existing project and risk management policies. This will reduce the resources necessary to conduct the assessment and spreads awareness of privacy throughout your organisation.

As part of their work in this area, they ICO commissioned a report into the use of PIAs and the potential for further integration with project and risk management. The report was provided by Trilateral Research and Consulting.

You can access the report and an executive summary here.

Annex 4 – Glossary

SaaS	Software as a Service
PaaS	Platform as a Service
IaaS	Infrastructure as a Service
PIA	Privacy Impact Assessment
ICT	Information and Communication Technology
NIST	National Institute of standards and technology
SLA	Service Level Agreement
DPS	Digital Public Services
BIL	Business Impact Level
ISO	International Organisation for Standardisation

Annex 5 – Related reading

- Scottish public sector High Level Operating Framework (HLOF) – published June 2013
- Scotland's Digital Future: Data Hosting and Data Centre Strategy for the Scottish Public Sector – Published Apr. 2014
- John McClelland's Review of ICT Infrastructure in the Public Sector in Scotland - published June 2011
- Scotland's Digital Future - Delivery of Public Services – published Sept. 2012
- National Institute of Standards and Technology (NIST) definition of Cloud Computing. – published Sept. 2011
- European Commission's European Cloud Computing Strategy – published Sept. 2013
- Cloud Security Alliance (CSA)
- Common Assurance Maturity Model (CAMM)
- FedRAMP (U.S. Federal Government)
- https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf– published Feb. 2013
- http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909494 – published Dec. 2011
- http://www.cesg.gov.uk/publications/Documents/is1_risk_assessment.pdf – published Oct. 2009
- https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/286667/FAQ2_-_Managing_Information_Risk_at_OFFICIAL_v2_-_March_2014.pdf – published Mar. 2014
- Information Commissioner's Office, Conducting privacy impact assessments code of practice – published Feb. 2014
- CESG Cloud Security Guidance – updated May 2014
- The European Data Protection Supervisor - The transfer of personal data to third countries and international organisations by EU institutions and bodies – published – published Nov. 2012

This publication is available at **www.gov.scot**

Any enquiries regarding this publication should be sent to us at
The Scottish Government
St Andrew's House
Edinburgh
EH1 3DG

ISBN: 978-1-78544-278-0 (web only)

Published by The Scottish Government, March 2015

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS47545 (03/15)