Advice Note: Considering Cloud Services

Supporting the *Public Service ICT Strategy*

December 2015

An Roinn Caiteachais Phoiblí
agus Athchóirithe
Department of Public
Expenditure and Reform

Introduction

A key objective of the *Public Service ICT Strategy*[1] focuses on improving governance around ICT in the Public Service. ICT governance ensures that ICT projects are aligned, directed, and monitored to support the specific goals and objectives of a Public Body at a whole-of-government level[2]. This is in line with the goals of the Public Service Reform Plan and supports the unification approach envisaged in the Civil Service Renewal Plan. To support this approach to governance, policies and advice are required to inform Public Bodies on individual ICT issues.

The Office of the Government Chief Information Officer (OGCIO) in the Department of Public Expenditure and Reform, working with the Public Service CIO Council, will develop a portfolio of policies and advice notes on key ICT issues to manage risk and support standardisation and integration. *Considering Cloud Services* provides advice to assist Public Bodies in making informed, risk-based decisions in relation to the adoption of cloud services.

Office of the Government CIO
Department of Public Expenditure and Reform
December 2015

[1] The aim of the *Public Service ICT Strategy*, approved by Government and published in January 2015, is to enable the Public Service use ICT to operate in a more efficient, shared and integrated manner across all of Government. It sets out five key strategic objectives to meet that aim. The Strategy is aligned with the objectives of the Public Service Reform Plan 2014 – 2016 and the Civil Service Renewal Plan and supersedes *eGovernment 2012 - 2015* and the 2012 Cloud Computing Strategy.

[2] In this context "whole-of-government" refers to non-commercial public bodies

1. Executive Summary

The term Cloud Services refers to information and communications technologies (ICTs) made available to users, over a network, on a pay-for-use basis (normally), by a Cloud Service Provider (CSP). Cloud Services are fully managed by the CSP and are designed to provide easy, scalable and on-demand access to a wide range of ICTs including business applications[3], information storage services (such as databases or file sharing services), communications services (such as email and social networking), or indeed entire data centres. Where the World Wide Web makes information available everywhere and to anyone, cloud computing makes computing power available everywhere and to anyone.

Cloud computing is a technological development that has been ongoing for some time and will continue to develop. Cloud services are now a recognised and maturing model for the delivery of ICT, and Public Bodies should consider the opportunities presented by the use of these services when developing business cases and making investment decisions around new business information systems.

Subject to a detailed risk assessment, cloud services should be considered potentially suitable for any category of public service information and especially that which is for the public domain. However, cloud services should not be considered for information classified as "Top Secret" as set out in Department of Finance *Circular 39/07 Classification of material as "top secret"*.

This paper aims to provide Public Bodies with advice to assist in making informed, risk-based decisions in relation to the adoption of cloud services in terms of the information and services to be entrusted to a CSP, including any government cloud services that may be implemented. Details on the plan for Government Cloud services will be available in early 2016. This is not an exhaustive guide but it does identify some of the key issues to be considered when evaluating Cloud deployment models, cloud service offerings and individual CSPs. It provides references to a number of established frameworks and tools that Public Bodies may find useful when assessing Cloud Services and CSPs.

Any decisions on the adoption of cloud services as a service delivery model, like for any ICT service, must be made by the Public Body itself based on an understanding of its own business requirements and approach. It will include a detailed assessment of the benefits, costs and risks of a range of possible alternatives. It will also consider issues such as risk aggregation and data aggregation concerns as well as other overriding factors such as relevant central policy direction.

[3] Bespoke business applications may not be suitable for Cloud provision. Public Service Bodies should also ensure that shared service offerings from the National Shared Service Office (NSSO) are availed of where appropriate and should engage with the NSSO in that regard.

2. Key Considerations for Adopting Cloud Services

Cloud computing consists of a set of technologies and service models that focus on network-based on-demand use and delivery of IT applications[4], processing capability, storage and memory space. The cloud services utilising these technologies and models can be delivered in-house or, more commonly, can be provided by an external service provider. They can be provided on a private or shared basis. Cloud services can also be provided exclusively for or by Government, referred to as the *Government Cloud*. The National Institute of Standards and Technology (NIST) in the USA has developed definitions for cloud computing which are generally accepted and used across the ICT industry and will be the definitions adopted by the OGCIO. The NIST definitions are described in Appendix A which also provides use-case considerations and more information on the Government cloud.

Using a cloud service as an outsourcing model provides many opportunities and advantages for Public Bodies. However, it also comes with risks that must be considered. Therefore, it is important to consider all elements of a public service, and its associated data, when considering its suitability for cloud service provision. Some key considerations for adopting cloud services:

1. As with any outsourced service, the adoption of cloud services to deliver your business can solve certain business problems and mitigate certain risks, while at the same time introducing other problems and risks. All risks need to be identified and managed appropriately from the outset.
2. Public Bodies must trust the Cloud Service Provider to provide a contractual level of service that may be vital for the running of the business. As such, key parts of the outsourcing decision include selecting a reputable CSP and ensuring service contracts cover any legal and regulatory obligations, business continuity requirements, as well as issues such as how data will be extracted from the CSP and what happens to any copies held by the CSP. Public Bodies should seek advice regarding the relevant jurisdiction that will apply for any legal issues that may arise.
3. A Cloud Service contract will be time-bound. Public Bodies need to consider their long-term strategy for the Cloud Service, including future requirements to move to a different CSP, or to deliver the service internally, and the associated costs and constraints. These should be built into the contract.
4. In moving multiple information systems or services to a single cloud service, Public Bodies should consider issues that may arise around risk aggregation and data aggregation.
5. Adopting cloud services will require Public Bodies to develop new skills focussed on the ability to manage the Cloud Service, both technologically and commercially.
6. The principles of data protection still apply to services or data moved to cloud services. Consequently, Public Bodies must ensure they continue to meet their legal obligations.
7. As with any planned expenditure, the requirements regarding public procurement still apply when procuring cloud services. The Office of Government Procurement (OGP) should be consulted as appropriate.
8. While a Public Body may be able to outsource the responsibility for the delivery of a service to the CSP, it cannot outsource its accountability for that service.

[4] This approach may not suit bespoke business applications.

4. A Decision-Making Approach for Cloud Adoption

When considering the implementation or acquisition of any new ICT system, Public Bodies should adopt a systematic approach to ensuring that all risks are properly identified and managed so that the expected business benefits are realised. The adoption of cloud services is no different and should follow the same assessment and governance process. This will typically include the steps set out below in addition to a Public Body's own existing governance model.

4.1 Understand the business requirements for the service you are planning

Identify the type of information or system you are considering moving to the cloud; is it data only, a business application, an entire business process or ICT infrastructure? Understand your business requirements, considering issues such as uptime, speed of deployment and on-going management overhead. What is the typical pattern of usage of the information system or data, for example does it peak at certain times and are those peaks predictable or seasonal? How can those peaks be accommodated?

Identify the nature and categorisation of the information that will be processed, stored or provided by the cloud service. Assess the business impact if that system or relevant data was compromised in some way, resulting in a loss of confidentiality, integrity or availability. Consider how the data is to be returned in a useable form at the end of the contract.

Particular care must be taken when considering moving personal data to a cloud service and the obligations set out in Data Protection legislation. Are you aware of your responsibilities as a data controller? How will the personal data be controlled? Do you have sufficient information regarding how, where and by whom the data is being processed/sub-processed?

It is important to note that the information or system may have very different confidentiality, integrity and availability requirements, and these characteristics should be assessed separately. For example, information in the public domain has no confidentiality requirements but may have very high availability requirements, making it ideal for placing in a public cloud service that can guarantee very high uptime.

Information confidentiality requirements are regularly cited as one of the main inhibitors to the adoption of cloud services. Many Public Bodies will have their own well-established systems for categorising the public service information for which they are responsible. They should however develop a mapping between their information categories and the various Cloud deployment models. Appendix B: "Categorisation of Information" addresses this issue in more detail, but the recommended approach can be summarised as follows:

Information Category		Appropriate for Cloud?
Top Secret	☒	Cloud is not an appropriate service delivery model (Circular 39/07 refers – see Note)
Information already in or planned for the public domain	☑	Take a Cloud-first approach
All other classes of information and information systems	?	Consider Cloud Services using advice in this document

Note: Cloud services should not be considered for information classified as "Top Secret" as set out in Department of Finance *Circular 39/07 Classification of material as "top secret"* – attached at Appendix C.

4.2 Identify the required Governance, Risk and Compliance (GRC) controls

Having considered the business requirements, the business impact and the nature of the information that will be transferred to the CSP, a risk assessment should be undertaken. Many Public Bodies will have their own established methodology for carrying out risk assessments, which should take into account the threats to the information or system, the likelihood of that threat occurring, as well as the business impact if the risk materialises. Public Bodies need also to be mindful of the legislative framework within which they operate, including but not limited to the legislation identified in Appendix H: "Legislative Framework".

All ICT implementations, whether cloud-based or not, are subject to risk. While it is important to be aware of and assess relevant risks, they should not be viewed as reasons not to adopt cloud services. Some of the more important cloud risks identified by the European Union Agency for Network and Information Security (ENISA) fall in to eight categories:

1. Loss of governance
2. Lock-in
3. Isolation failure
4. Compliance risks
5. Application security
6. Data Protection
7. Insecure or incomplete data deletion
8. Malicious insider

Note that many of these same considerations also apply where a Public Body is hosting a service internally.

In addition to the specific ENISA categories, other issues such as skills availability (within the Public Body and the CSP) and licensing arrangements need to be assessed. Public Bodies also need to ensure that the Cloud Services under consideration are capable of supporting their preferred technologies.

Appendix D: "Governance, Risk and Compliance Considerations for Cloud" provides more information on each of these categories.

The outcome of the risk analysis will help identify what controls are required to mitigate these risks. Public Bodies should then determine to what extent these controls are implemented or made available by the CSP within the selected service model. Consider whether the CSP can provide evidence that the required controls are being implemented correctly and are supported by appropriate policies and procedures. This should be provided on an ongoing basis through an agreed regular reporting process.

Having assessed the level of assurance of the CSP's GRC controls and having determined whether or not any residual risks are acceptable, consider additional mitigations that your organisation may need to implement to manage any remaining risks to acceptable levels. Appendix E: "Considerations for Assessing Cloud Services" provides more advice on the assessment of CSPs and their GRC controls.

4.3 Ask key questions

Key questions Public Bodies should ask Cloud Service Providers include:

1. What will the CSP do with your data?
2. Who can access your data and under what circumstances? Have CSP staff been properly trained and vetted?
3. Will third-party vendors have access to your data and under what circumstances?
4. Who ensures that data is protected within computer systems?
5. What encryption mechanisms does the CSP offer?
6. With what, if any, industry standards does the CSP's security architecture comply?
7. What happens to your data after the Cloud Service comes to an end?
8. Where will your data be processed?
9. What measures are used to safeguard customer data that is transferred outside the State and/or the EEA?
10. What measures are in place to prevent customer data being transferred outside the State and/or the EEA if that is a requirement?

4.4 Validate the business case

Public Bodies should develop and document a business case that identifies and quantifies the business and ICT drivers for moving to a cloud service. This should include an assessment of the cloud service against other alternative service delivery models, for example maintaining the service on-premises. This analysis should recognise the shift from capital expenditure to operational expenditure that comes with adopting cloud services as well as the new management skills required to oversee the CSP while also maintaining traditional ICT systems.

4.5 Manage the transition

A comprehensive project plan to manage the transition to, or adoption of the cloud service should be developed, taking into account any requirements to maintain continuity of service during the transition period. This plan should include the implementation of any information security controls identified as part of the risk assessment. Equally as important is to develop a plan to manage a transition off the cloud service.

5. Government Cloud

> **Delivery of Services via a Government Private Cloud**
> "Creating shared centres of excellence for the delivery and management of common technology infrastructure as a set of services to the wider Public Service. These would be internally and/or externally hosted and delivered via a secure Government Cloud network. Services include hosting, email, web monitoring, servers and storage. These services would be delivered and operated from a number of centres…"
>
> – Public Service ICT Strategy

The "Build to Share" stream of the Public Service ICT Strategy focuses on the sharing of services across Public Bodies delivered through a government cloud to drive efficiency, reduce cost and support integration across the Public Service. The ICT base-lining exercise undertaken in 2015, highlights the potential gains from rationalising the instances of Government data centres and smaller computer rooms into a Government Cloud service which can lower running costs and deliver more resilient, robust and capable ICT infrastructure and services.

Consideration of migration to Government Cloud services will be one of the options available to Public Service Bodies as they consider how to implement their ICT services. Details on the plan for Government Cloud services will be available in early 2016.

6. In Summary

Cloud services should be considered a valid and increasingly mature service delivery model for ICT services in support of business requirements. Cloud service models are no different to any other model in that the adoption of cloud services should follow the established governance and risk assessment processes within Public Bodies, including the development of a documented business case that assesses cloud along with other options for ICT service delivery.

Cloud services should be viewed as another model of outsourcing and the same due diligence applied to the selection of the Cloud Service Provider and the agreement of contract terms as for any other outsourcing decision. As with any outsourcing arrangement, a Public Body needs to be aware that it cannot outsource its accountability for services delivered through cloud services. Public bodies need to take particular care in meeting obligations regarding personal data, in line with Data Protection legislation, and should also be aware of issues around risk aggregation or data aggregation. Many of the same considerations apply to hosting a service internally.

A Government Cloud service will be delivered as part of the Build to Share stream of the Public ICT Strategy and will be available to Public Bodies to draw down a range of ICT services. Details on services and delivery models offered via the Government Cloud will issue separately.

The following Appendices provide more detailed advice to help Public Bodies make informed, risk-based decisions in relation to the adoption of Cloud Services. They identify the issues to be considered in evaluating and assessing Cloud deployment models, Cloud Service offerings and individual Cloud Service Providers. A sample high-level decision-tree for adopting Cloud Services is also provided in Appendix F.

The information provided is not intended to be exhaustive and should be used in conjunction with a suitable risk assessment framework and security assessment (examples are provided in Appendix G: "Common Risk Assessment Frameworks"), as part of a thorough due diligence process.

Public bodies must satisfy themselves that any system and associated data is provisioned in the most effective and robust fashion with due regard to risks and mitigation measures, both internal and external.

Appendices

Appendix A: Cloud Definitions and Use-Case Considerations

National Institute of Standards and Technology

The National Institute of Standards and Technology in the US (NIST) have developed the following definitions for Cloud computing which are generally accepted and used across the ICT industry. See also http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

The 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.

Essential Characteristics:

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.

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).

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 datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

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.

Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability[5] 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.

Service Models:

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[6] including network, servers, operating systems,

[5] Typically this is done on a pay-per-use or charge-per-use basis.

[6] A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components.

storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.

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[7]. 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.

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).

Deployment Models:

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

Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations 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 organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

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 organization, or some combination of them. It exists on the premises of the cloud provider.

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 standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

The European Union Agency for Network and Information Security (ENISA) also provides definitions for Cloud Services and deployment models in its guidance material. These can be found at: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing.

Although not specifically identified in the NIST categories, a number of Cloud vendors have introduced the concept of a Virtual Private Cloud (VPC). This involves utilizing public Cloud infrastructure in a

The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.

[7] This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.

private or semi-private manner and interconnecting these resources to the internal resources of the customer's datacentre, usually via a virtual private network (VPN).

In addition to the service models above, new service models are emerging, including for example: Communication (or Connectivity) as a Service (CaaS), Computing as a Service (CompaaS), and Data Storage as a Service (DSaaS). These may be of interest as their definition and offerings mature.

Use-case considerations for Cloud Service models

When considering Cloud adoption, Public Bodies will need to consider which Cloud Service models, (SaaS, PaaS or IaaS) may be most appropriate. An important differentiator between these service models is the degree to which the Cloud Service consumer is responsible for implementing and managing the security of the Cloud Service. The Cloud Security Alliance summarises these as follows:

> "In SaaS environments the security controls and their scope are negotiated into the contracts for service; service levels, privacy, and compliance are all issues to be dealt with legally in contracts. In an IaaS offering, while the responsibility for securing the underlying infrastructure and abstraction layers belongs to the provider, the remainder of the stack is the consumer's responsibility. PaaS offers a balance somewhere in between, where securing the platform falls onto the provider, but both securing the applications developed against the platform and developing them securely, belong to the consumer."

The technology, service models and contract arrangements surrounding Cloud Services are constantly evolving, so the following advice is of necessity general and based on Cloud Service offerings at the time this document is issued.

Software as a Service:
SaaS service models will be most appropriate in the following circumstances:

- Where the business process under consideration fits easily within the standard business processes provided within the SaaS solution;
- Where the business process is largely independent or where there are no interdependencies or interfaces to other business processes within the organisation that would require changes to the standard SaaS solution;
- The organisation only needs control over who has access to the solution, and does not need to control the SLAs, maintenance windows, or underlying architecture.

Platform as a Service:
PaaS service models will be most appropriate in the following circumstances:

- Where applications and workflows may need to be configured specifically to the requirements of the organisation;
- Where the application is independent of any technology "stack", (i.e. operating system, database, application server or programming language);
- Where the organisation needs to focus more on building business functionality than architecting a specific technical solution;
- Where the organisation does not need to control the SLAs, maintenance windows, or underlying architecture.

Infrastructure as a Service:
IaaS service models will be most appropriate in the following circumstances:

- Where the application is independent of any particular hardware requirement;

- Where an organisation has a requirement for the characteristics of Cloud Services, including on-demand resources, rapid elasticity and metered price consumption, while retaining control over the architecture and security of the solution.

In some circumstances the additional controls available to the Cloud Service customer may make Infrastructure as a Service offerings more attractive to Public Bodies for information systems or data with more stringent security requirements.

Government Cloud

> **Delivery of Services via a Government Private Cloud**
> "Creating shared centres of excellence for the delivery and management of common technology infrastructure as a set of services to the wider Public Service. These would be internally and/or externally hosted and delivered via a secure Government Cloud network. Services include hosting, email, web monitoring, servers and storage. These services would be delivered and operated from a number of centres…"
>
> – Public Service ICT Strategy

The "Build to Share" stream of the Public Service ICT Strategy focuses on the sharing of services across Public Bodies delivered through a Government Cloud to drive efficiency, reduce cost and support integration across the Public Service. The ICT base-lining exercise undertaken in 2015, highlights the potential gains from rationalising the instances of Government data centres and smaller computer rooms into a Government Cloud service which can lower running costs and deliver more resilient, robust and capable ICT infrastructure and services.

Consideration of migration to Government Cloud services will be one of the options available to Public Service Bodies as they consider how to implement their ICT services. Details on the plan for Government Cloud services will be available in early 2016.

Appendix B: Categorisation of Information

Privacy and confidentiality are the most common concerns when considering a move to the Cloud, particularly when the information system or data includes personal or otherwise sensitive data. Such data should be identified through proper information categorisation prior to migration, and appropriate risk controls implemented to protect against unauthorised disclosure.

Many Public Bodies will have their own well-established systems for categorising the public service information for which they are responsible. They should however develop a mapping between their information categories and the various Cloud deployment models, using the following as guidance:

Information Category		Appropriate for Cloud?
Top Secret	☒	Cloud is not an appropriate service delivery model (Circular 39/07 refers – see Note)
Information already in or planned for the public domain	☑	Take a Cloud-first approach
All other classes of information and information systems	?	Consider Cloud Services using advice in this document

Note: Cloud Services should not be considered for information classified as "Top Secret" as set out in Department of Finance *Circular 39/07 Classification of material as "top secret"* – see Appendix C.

Public Bodies that have not already done so should consider adopting an information categorisation system for all their public service information.

Specifically in relation to Personal Data, the Data Protection Commissioner has issued useful guidance in relation to data protection in the cloud and identifies three issues that need to be considered regardless of the Cloud Service model or deployment model[8]. These can be summarised as:

1. *The security of the data.* The Data Protection Acts place responsibility for data security squarely on the data controller who is accountable to the individual data subject for the safeguarding of their personal information. A data controller must therefore be satisfied that personal data will be secure if it is outsourced to a Cloud Service Provider, recognising the principle that accountability for the security of the data cannot be outsourced.
2. *The location of the data.* Personal data that is held within the European Economic Area (EU Member States plus Iceland, Liechtenstein and Norway) benefits from a common standard of protection laid down at EU level. When data is transferred outside of the EEA, special measures must be taken to ensure that it continues to benefit from adequate protection.
3. *The requirement for a written contract.* The Data Protection Acts require that there be a written contract with the CSP and any sub-processors setting out their obligations in respect of data protection.

Notwithstanding the above, a significant proportion of data processed by Public Bodies, including personal data can be considered suitable for migration to Cloud Services, subject to appropriate security controls and contract conditions being in place. The ultimate decision however rests with the Public Body, based on their assessment of the benefits, costs and risks associated with the Cloud Service.

[8] http://www.dataprotection.ie/viewdoc.asp?m=m&fn=/documents/press/Cloudcomputing.htm

Appendix C: Circular 39/07 Classification of material as "top secret"

The Circular is also available at: http://circulars.gov.ie/pdf/circular/finance/2007/39.pdf

E159/29/07

14 December 2007

To all Accounting Officers

Circular 39/07: Classification of material as "top secret"

A Dhuine Uasail

I am directed by the Minister for Finance to refer to Circular 20/98 concerning the classification of material as "top secret" and to say that Circular 20/98 is now superseded by this Circular.

1. Classifying Top Secret Material

The responsibility for classifying material as "top secret" lies with the Department in which the material originated or was initially received. In determining whether information, documentation (including images, audio, video, web content etc), data, knowledge etc. is to be classified as "top secret", Departments need to consider if the release of the material would

- Put at risk the life or safety of any individual;
- Pose a serious threat to the security, defence or international relations of the State;
- Undermine the policing or judicial or other processes involved in dealing with serious crime;
- Pose a serious threat to the economic interests of the State;
- Adversely affect developments in relation to Northern Ireland.

The classification of "top secret" should be applied only where essential. Excessive usage of "top secret" is likely to debase the classification and lessen its effectiveness. Limited usage of the classification will also serve to underline the truly exceptional nature of the material so classified. Departments should ensure that documents derived from such "top secret" material e.g. excerpts, paraphrases, summaries, references are similarly classified, where appropriate.

2. Protection of "top secret" information

It is important that where material is classified as "top secret", particular measures are taken to ensure its protection. Where material would not warrant special protection, by definition it should not be classified as "top secret". It is not possible to be prescriptive about the manner in which Departments should protect information deemed to be "top secret". Arrangements will, of necessity, vary both between, and even within, Departments depending on the nature of the material e.g. the reason for its "top secret" classification, the number and grades of individuals who must have access to the material in the course of their work, the incidence of such access, etc. Nonetheless, it is essential that access to top secret documents is restricted to appropriate people. At minimum the arrangements should encompass the following –

- the storage of material (including removable electronic media) in a locked safe or departmental strong room with access restricted to a limited number of nominated people;
- the maintenance of confidential file indexes and tables of file contents for all "top secret" material;
- the availability of material for consultation only, and under the direction of a nominated officer of senior rank;
- the application of unique identifiers to any copies made so that such copies can be traced back to their original;
- the maintenance of a register of individuals who access any item of such material (including copies), recording the date and time of such access, the date and time of the material's subsequent return to safe-keeping, and the signature of the officer accessing the material.

This list is not exhaustive and Departments are free to adopt other measures which they deem to be appropriate. The arrangements deemed appropriate should be fully documented and formally approved by the Secretary General. These arrangements and the classification of material as "top secret" should be reviewed regularly.

3. Use of Computers and Electronic Storage Media

The preparation and storage of "top secret" material on computers poses particular difficulties that Departments must address. For example, because of the way computers typically use storage media, it can be difficult to ensure that a document is completely deleted. It is imperative that Departments put protocols and arrangements in place that take account of these difficulties. In particular, the protocols and arrangements should address –

- the physical security of the computer(s) on which "top secret" documents are created;
- the physical protection of electronic storage media used for the storage of "top secret" documents when not in active use;
- the provision of facilities that limit access to authorised personnel only;
- the need to completely delete documents, including temporary copies maintained by the application or by the operating system;
- the necessity or otherwise for encryption of "top secret" material;
- the indexing of "top secret" documents held electronically;
- the logging of all access to electronic storage media which contain "top secret" documents; and
- the physical destruction and disposal of electronic storage media at end-of-life.

4. Freedom of Information

It should be noted that any requests for a record classified as "top secret" fall to be considered in accordance with the provisions of the Freedom of Information legislation.

Mise, le meas,

Jim Duffy,

Assistant Secretary

Appendix D: Governance, Risk and Compliance Considerations for Cloud

Public Bodies need to be aware of the risks that can arise when adopting and managing a Cloud Service and a Cloud Service Provider (CSP). Note that many of these issues are applicable to internal provisioning also.

While it is important to be aware of and assess these risk areas, they should not be viewed as reasons not to adopt Cloud Services. The impact of a migration to the Cloud depends on the Cloud Service model and deployment model being considered. Many of the risks are particularly relevant to public Software as a Service (SaaS) Cloud offerings, and may not arise in the case of private or community Clouds, or in Infrastructure as a Service (IaaS) offerings. In addition, risks can be mitigated through the use of compensating controls or technologies, such as appropriately classifying data for migration to the Cloud, or the use of data encryption techniques.

All ICT implementations, whether Cloud based or not are subject to risk and require proper assessment and management of those risks. In some circumstances the adoption of Cloud Services will reduce overall risk as the CSP may be able to offer levels of service and availability that a PSB by itself would not have the resources to achieve.

A number of risk assessment frameworks have been developed to assist organisations in their decisions to move to the Cloud, including frameworks from the NSAI, the Cloud Security Alliance (CSA), ENISA, ISACA and NIST. References to these frameworks are included in Appendix G: "Common Risk Assessment Frameworks" and Public Bodies should assess whichever framework best suits their requirements.

These frameworks identify key governance issues that need to be considered in making decisions to adopt Cloud Services. ENISA has summarised what it considers to be the most important Cloud risks into the following eight categories:

1. *Loss of governance:* in using Cloud infrastructures, the Cloud Service Customer (CSC) cedes control to the CSP on a number of issues that may affect governance and enterprise risk management. At the same time, Service Level Agreements (SLAs) may not offer a commitment to provide such services on the part of the CSP. For example, procedures for incident detection, response, notification, investigation and remediation may not be included in the SLA. In addition the CSC may not be able to assess how risks are managed within the CSP, or audit compliance against control objectives.

2. *Lock-in:* a lack of tools, procedures or standard data formats or services interfaces that could guarantee data, application and service portability. This can make it difficult for the CSC to migrate from one provider to another or migrate data and services back to an in-house IT environment. CSCs are particularly exposed in the event of the business or technical failure of a CSP and may be wholly dependent on the CSP's business continuity plans and capabilities, unless the CSC has implemented its own Business Continuity and Disaster Recovery plans.

3. *Isolation failure:* multi-tenancy and shared resources are defining characteristics of Cloud computing. This risk category covers the failure of mechanisms separating storage, memory, routing and even reputation between different tenants. Isolation failure could also extend to physical security, as computing resources are shared with other tenants, so if physical access to the CSP's infrastructure is provided to one tenant, they could potentially access information systems or data of other tenants.

4. *Compliance risks:* investment in achieving certification (e.g., industry standard or regulatory requirements) may be put at risk by migration to the Cloud, particularly if the CSP cannot provide

evidence of their own compliance with the relevant requirements or if the CSP does not permit audit by the CSC. Other compliance issues could include the inability to respond in a timely manner to electronic discovery requests, or data breach notification requirements.

5. *Application security:* Particularly in the case of SaaS, the CSC has little or no control over the Software Development Life Cycle and the secure coding techniques adopted by the CSP. Equally the CSC has no control over the release cycle of application upgrades. CSC management interfaces of a public Cloud service may be accessible through the Internet and mediate access to larger sets of resources (than traditional hosting providers) and therefore pose an increased risk, especially when combined with remote access and web browser vulnerabilities.

6. *Data protection:* Cloud computing poses several data protection risks for CSCs and CSPs. In some cases, it may be difficult for the CSC (in its role as data controller) to effectively check the data handling practices of the Cloud provider, including data transfers to other jurisdictions, (in particular transfers outside of the EEA), and thus to be sure that the data is handled in a lawful way. Is the CSP able to provide access logs for records containing personal data?

7. *Insecure or incomplete data deletion:* when a request to delete a Cloud resource is made, as with most operating systems, this may not result in secure erasing of the data. Adequate or timely data deletion may also be impossible (or undesirable from a customer perspective), either because extra copies of data are stored but are not available, or because the disk to be destroyed also stores data from other clients. In the case of multiple tenancies and the reuse of hardware resources, this represents a higher risk to the CSC than with dedicated hardware.

8. *Malicious insider:* while usually less likely, the damage that may be caused by malicious insiders is often far greater. Cloud architectures necessitate certain roles that are extremely high-risk. Examples include CSP system administrators and managed security service providers.

Additional considerations:

Skills – Public Bodies need to be mindful of the additional skills that they may need to develop to effectively assess and manage these governance, risk and compliance issues. They may also need to develop the technical and commercial skills required to understand the services offered and to manage the CSP contract and pricing models so that value for money is maintained throughout the contract lifecycle. In parallel, Public Bodies need to ensure that the Cloud Services under consideration are capable of supporting their preferred technologies.

Licences – The implications for licensing and for ensuring licensing compliance within or across environments also should be assessed.

Appendix E sets out general advice to assist in assessing Cloud Service Providers and the Cloud Services they offer.

Appendix E: Considerations for Assessing Cloud Services

The following gives general advice to assist in assessing Cloud Services. However, Public Bodies should refer to particular guidance, as it emerges, from the Office of Government Procurement (OGP) on procuring Cloud Services.

Contract and Service Management

In dealing with Cloud Service providers (CSP), a Public Body should request detailed contract and service management information to help them assess all aspects of the service offering. This may include for example:

- Details of proposed Service Level Agreements (SLAs), downtime calculations, details of service credits or penalties and exclusion provisions;
- Support arrangement, response times and escalation procedures;
- Details of Business Continuity arrangements;
- Minimum contract durations and the mechanisms and costs associated with early termination of contracts;
- How is access to the data controlled and authorised?
- Details of arrangements for migrating data and business applications out of the Cloud/ platform, including obligations of the CSP regarding safe deletion of all data after it has been moved from the CSP, and possible removal of audit trail / log data;
- How can the service contract be amended – by whom and how? How are changes communicated?
- Details of pricing models used and variables;
- How the Cloud Service Provider (CSP) complies with Data Protection legislation, including location of data;
- Governing law and jurisdiction – Public Bodies should seek advice regarding the relevant jurisdiction that will apply for any legal issues that may arise;
- Details of how 3rd parties or sub-processors are managed and controlled;
- Details of how data access requests by law enforcement are handled;
- Incident response processes;
- Litigation response processes;
- Details of how integration with existing systems is to be achieved, including integration of authentication mechanisms.

The level of detail required will depend on the type of data concerned – transfers of critical and sensitive information will require more consideration than transfers of low value and non-critical data.

Certification

A Public Body will also want assurance in relation to the CSP's governance, risk, compliance (GRC) and security processes and controls. This would typically be achieved by way of a detailed technical analysis incorporating an audit of the CSP. However in many cases a CSP will not agree to a direct "right to audit", so Public Bodies may need to rely on 3rd party certifications or audits. Certification schemes can provide a level of confidence in CSPs. A CSP itself can be certified (cloud provider certification) as can the individual Cloud Service offerings of the CSP (cloud service certification). The European Union Agency for Network and Information Security (ENISA) has developed a Cloud Certification Schemes List (CCSL)[9] which gives an overview of different existing certification schemes which could be relevant for cloud computing customers. CCSL also shows the main characteristics of

[9] https://resilience.enisa.europa.eu/cloud-computing-certification

each certification scheme. ENISA has also developed a Cloud Certification Schemes Metaframework (CCSM) as an extension of the CCSL. The goal of the meta-framework is to provide a neutral high-level mapping from the customer's Network and Information Security requirements to security objectives in existing cloud certification schemes, which facilitates the use of existing certification schemes during procurement.

ENISA also provides an online tool[10] that allows customers to choose a set of relevant security objectives, to see which of these security objectives are addressed by which cloud certification schemes (and also in more detail where each objective is addressed). The online tool also allows customers create a number of custom forms and checklists for procurement as tools in their procurement process (for example as checklists for evaluating offers or as the basis for questionnaires).

Some other certification or assessment considerations:

- Certifications such as ISO/ IEC 27001, 27002, 27005 etc. (being careful to consider the scope of such certifications). ISO/ IEC 27018, which builds on ISO 27001 and 27002, provides guidance to CSPs on protecting the personally identifiable information (PII) of their customers and on implementing measures for protecting PII.
- SSAE 16 SOC Reports[11] are independent assessments of internal controls within a service organisation. In particular SOC2 reports focus on controls relevant to security, availability, processing integrity, confidentiality, or privacy. A Type I report looks at policies and procedures in operation as of a specified point in time, whereas a Type II report is an assessment of the policies and procedures in operation, including tests of operating effectiveness for a period of time.
- STAR assessments[12] range from Level 1, a self-assessment by the CSP, to Level 2, which is an assessment carried out by an independent third party, to Level 3 which is currently under development and will involve continuous auditing/ assessment of the security practices of the CSP.
- The US Government's Federal Risk and Authorization Management Program (FedRAMP)[13], which runs a programme that provides a standardised approach to security assessment, authorisation, and continuous monitoring for cloud products and services.
- The Cloud Security Alliance have developed an assessment questionnaire[14] (the Consensus Assessments Initiative Questionnaire or CAIQ) which is useful in assisting customers in vetting CSPs on the security of their offering and their overall security profile. This questionnaire is based on 16 governance and operating domains sub-divided into more detailed control areas. In addition, this questionnaire cross-references other major security and governance frameworks, including the ENISA Cloud Computing Information Assurance Framework, ISO/IEC 27001:2013, Cobit 5.0, PCI DSS 3.0 and the EU Data Protection Directive. Again, some CSPs self-assess against this CAIQ and make these assessments publicly available.

[10] https://resilience.enisa.europa.eu/cloud-computing-certification/list-of-cloud-certification-schemes/cloud-certification-schemes-metaframework

[11] Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organisation and Service Organization Control (SOC) Reports

[12] The Cloud Security Alliance Security, Trust & Assurance Registry

[13] https://www.fedramp.gov/marketplace/compliant-systems

[14] https://Cloudsecurityalliance.org/download/consensus-assessments-initiative-questionnaire-v3-0-1

- The Article 29 Data Protection Working Party[15] publishes opinions and recommendations on various data protection topics from time to time, including on issues such as the adequacy of legal frameworks underpinning international data transfers carried out internally within CSPs.

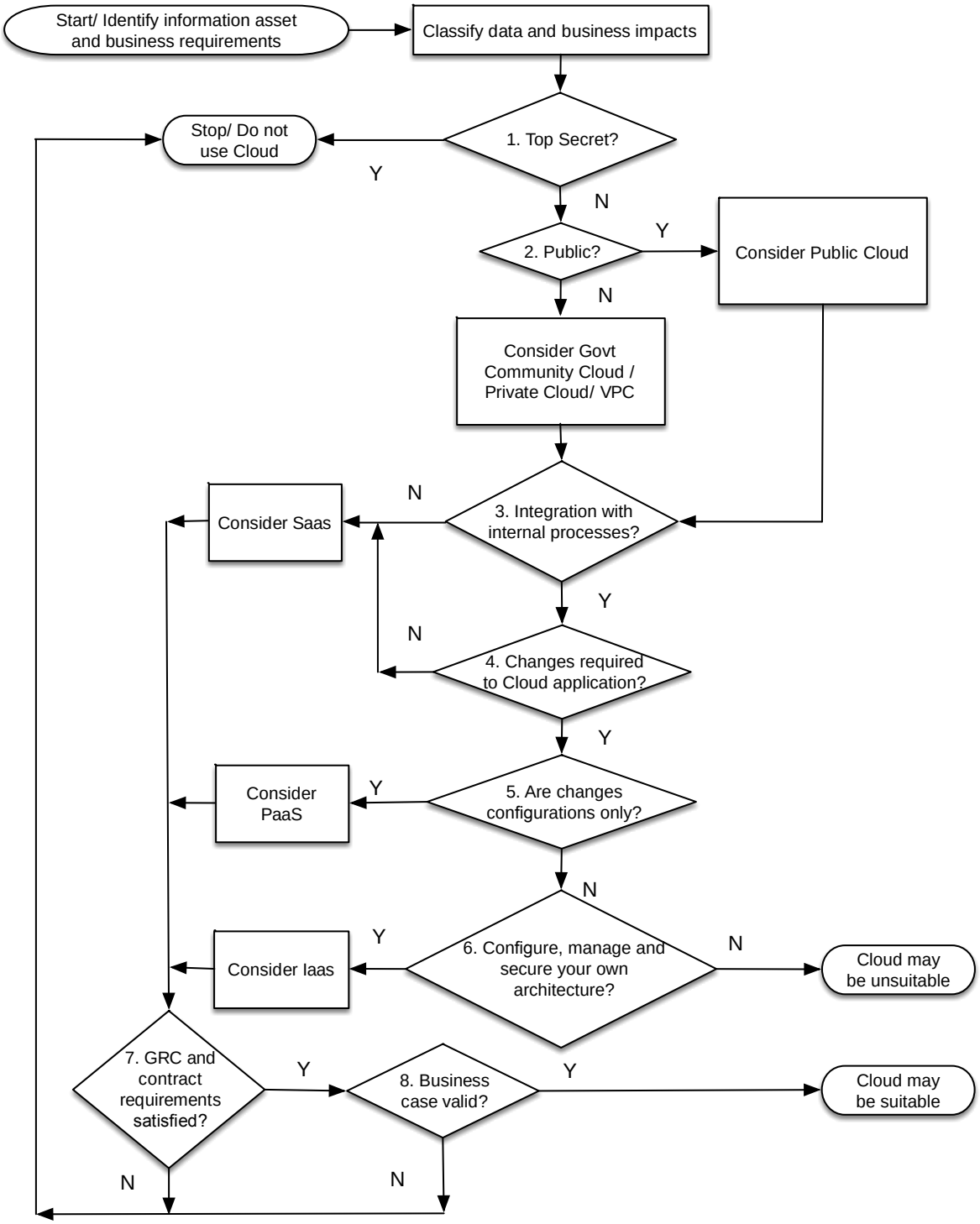
Many CSPs publish certifications on their websites for public inspection. Where none of these independent assessments are available or do not fully address the areas of concern, Public Bodies should conduct their own evaluation of the GRC controls provided by the CSP.

Again, this advice is of necessity general and based on Cloud Service offerings at the time this document is issued.

[15] The Article 29 Working Party is composed of representatives of the national data protection authorities (DPA), the EDPS and the European Commission

Appendix F: A Sample Decision Tree for Adopting Cloud Services

Taking the advice in this document into consideration, the following is a high-level decision-tree for adopting Cloud Services.



Breakdown of Cloud Services decision tree:

Decision	Answer	Description	Next Step
1. Is the information Top Secret?	Yes	If the information is categorised as Top Secret then Cloud Services must not be used.	Solution: Stop - do not use Cloud Services
	No	If the information is not Top Secret Cloud Services can be considered.	2. Is the information Public?
2. Is the information Public?	Yes	If the information is Public then Public Cloud Services can be used.	3. Integration with internal processes?
	No	If the information is not Public, then Cloud Services can still be considered.	Action: Make a risk-based assessment of the suitability of Cloud Services such as Government Community Cloud / Private Cloud/ VPC, considering also their location.
3. Integration with internal processes?	Yes	If there are integration points with internal business processes or systems, these may not be compatible with a standard SaaS Cloud Service.	4. Changes required to Cloud application?
	No	A standard SaaS Cloud Service may meet the business requirement.	Consider SaaS. 7. GRC and contract requirements satisfied?
4. Changes required to Cloud application?	Yes	If there are changes required to the standard application to implement the desired business requirement, these may not be compatible with a SaaS Cloud Service.	5. Are changes configurations only?
	No	A standard SaaS Cloud Service may meet the business requirement.	Consider SaaS. 7. GRC and contract requirements satisfied?
5. Are changes configurations only?	Yes	If the required changes are configurations rather than customisations of a standard application, a PaaS Cloud Service may fulfill the business need.	Consider SaaS. 7. GRC and contract requirements satisfied?
	No	You may need more control over the architecture of the solution than is provided by SaaS or PaaS.	6. Configure, manage and secure your own architecture?
6. Configure, manage and secure your own architecture?	Yes	If you need to have control over the architecture of the solution, including OS, application software, security configuration etc, then consider IaaS.	Consider IaaS. 7. GRC and contract requirements satisfied?
	No	If you have specific hardware requirements, or for some other reason neither IaaS, PaaS nor SaaS meet your requirements, a Cloud Service will not be appropriate for your needs.	Solution: A cloud solution is probably not the best solution for your business needs.

/continued

Decision	Answer	Description	Next Step
7. GRC and contract requirements satisfied?	Yes	If the CSP can be proven to meet all your GRC and contract requirements, then their Cloud Service may be suitable.	8. Business case valid?
	No	If the CSP cannot satisfy your GRC and contract requirements, then you should not progress with the Cloud Service.	Solution: Do not use Cloud Services
8. Business case valid?	Yes	The business case for Cloud Services is valid, having considered all your requirements and having assessed the Cloud Services against other alternative service delivery models.	Solution: Cloud Services may be suitable.
	No	The business case for Cloud Services is not valid, compared to other alternative service delivery models.	Solution: Do not use Cloud Services

Appendix G: Common Risk Assessment Frameworks for Cloud Adoption

NIST Guidelines on Security and Privacy in Public Cloud Computing

http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

ENISA Cloud Computing Information Assurance Framework

https://www.enisa.europa.eu/activities/risk-management/files/deliverables/Cloud-computing-information-assurance-framework

Cloud Security Alliance Security Guidance for Critical Areas of Focus in Cloud Computing v3.0

https://Cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-focus-in-Cloud-computing-v3

Cloud Security Alliance Consensus Assessments Initiative Questionnaire

https://Cloudsecurityalliance.org/download/consensus-assessments-initiative-questionnaire-v3-0-1

ISACA Security Considerations for Cloud Computing (ISACA members only)

http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/security-considerations-for-Cloud-computing.aspx

The EU's Article 29 Working Party, in its Opinion 5 /2012 sets out in detail the data protection issues that need to be addressed both by users of Cloud Services and providers of these services

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

The NSAI has published a recommendatory document SWiFT 10:2012 Adopting the Cloud - decision support for cloud computing

http://shop.standards.ie/nsai/details.aspx?ProductID=1524024

Appendix H: Legislative Framework

The following is a non-exhaustive list of the legislative and regulatory framework of relevance to Public Bodies considering the adoption of Cloud Services.

- Official Secrets Act, 1963
- The Data Protection Act, 1988 and the Data Protection (Amendment) Act 2003
- Copyright and Related Rights Acts 2000 to 2007.
- The Freedom of Information Circular 7/98 and Acts 1997 to 2014
- The Electronic Commerce Act, 2000
- National Archives Act, 1986

as well as a range of Criminal Justice legislation.

Appendix I: Abbreviations

Terms

CSC	Cloud Service Customer
CSP	Cloud Service Provider
GRC	Governance, Risk, Compliance
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
SaaS	Software as a Service
SLA	Service Level Agreement
VPC	Virtual Private Cloud

Organisations

CSA	Cloud Security Alliance https://cloudsecurityalliance.org/
ENISA	European Union Agency for Network and Information Security https://www.enisa.europa.eu/
ISACA	Information Systems Audit and Control Association http://www.isaca.org/chapters5/Ireland/Pages/default.aspx
NIST	National Institute of Standards and Technology (US) http://www.nist.gov/
NASI	National Standards Authority of Ireland https://www.nsai.ie/