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

Cloud Computing Advice Note

October 2019

Prepared by the Office of the
Government Chief Information Officer

Contents

Cloud Computing Advice Note

> **Organisations should no longer decide *whether* to move to cloud for new or existing systems. The decision to be made now is *what, how* and *when* to move to cloud.**

1. Introduction

In December 2015 *Considering Cloud Services* was issued in line with the Public Service ICT Strategy. It provided advice to assist public service organisations in making informed, risk-based decisions in relation to the adoption of cloud services. While much of the advice in *Considering Cloud Services* is still valid, this new advice note recognises that the world of cloud computing, as well as the policy and legislative environments, have developed rapidly since. Moreover, it is clear that the industry has matured in terms of the viability and benefits of cloud adoption. Consequently, the Government believes that it is an opportune time for a more proactive and progressive approach to embracing cloud computing.

In general, it continues to be the case that cloud computing services should be considered potentially suitable for any category of public service information or system except where such data would be classified as 'top secret' as per Circular 39/07[1]. Consequently, all new government systems should be developed to exploit the opportunities presented by cloud deployment, where possible, and all existing systems will be reviewed for cloud capability. Systems should move to public cloud or government private cloud environments over time and where practicable. In all cases, a move to cloud will be a business decision on the basis of specific considerations made by individual public service organisations.

This note aims to provide high-level guidance to assist organisations in making decisions in relation to the adoption of cloud services. It does not go into the technical and functional features of the infrastructure provided to supply a cloud computing environment nor does it recommend particular providers, products or solutions.

As set out previously, while organisations may outsource their responsibility for the delivery of a service to a cloud service provider, they cannot outsource their accountability for that service. In addition organisations remain fully responsible regarding their regulatory

[1] https://assets.gov.ie/16354/836258897a554bb4ab9676aab0e31b17.pdf

obligations including data protection. Consequently, organisations will need to put in place or update their own local cloud strategy, plans and policies.

This cloud advice note has been developed by the Office of the Government Chief Information Officer (OGCIO) in the Department of Public Expenditure and Reform in conjunction with the ICT Advisory Board and with input also from the wider public service ICT community. In addition, it takes into consideration input from a public consultation that took place towards the end of 2018 which afforded industry, academia and members of the public to input their views.

2. Definitions

While a number of popular definitions of cloud computing exist there is no overarching agreed definition as cloud computing refers to a concept comprising a set of combined technologies and not to a specific technology.

The United States National Institute of Standards and Technology (NIST) definition of Cloud Computing[2] identifies for its cloud model five essential characteristics, three service models (Software as a Service - SaaS; Platform as a Service - PaaS; and Infrastructure as a Service - IaaS) and four deployment models: public, private, community and hybrid (a composition of the former three models) cloud environments. Although issued in September 2011, the NIST definition is still generally accepted even as the range and scope of technology solutions offered “as a service” continues to develop.

In Europe, the European Union Agency for Network and Information Security (ENISA), which has a particular focus on network and information security, issued a series of cloud related publications targeted mostly to supporting public bodies in the EU[3].

The OECD, in its 2014 report, *Cloud Computing: The Concept, Impacts and the Role of Government Policy*[4], discusses the *characteristics* of cloud computing, cloud usage and service models, and cloud deployment models.

For the purpose of this advice note, cloud computing consists of a set of technologies and service models that focus on network-based on-demand use and delivery of IT applications, processing capability, storage and memory space. The cloud services utilising these technologies and service models can be provided by an external service provider or can be

[2] https://csrc.nist.gov/publications/detail/sp/800-145/final
[3] https://www.enisa.europa.eu/topics/cloud-and-big-data
[4] https://www.oecd-ilibrary.org/science-and-technology/cloud-computing-the-concept-impacts-and-the-role-of-government-policy_5jxzf4lcc7f5-en

delivered in-house or a combination of both. They can be provided on a private or shared basis.

3. Business Context

The pace of and demand for digitalisation is accelerating and the way in which government adopts the infrastructure required to support new technologies needs to change. Traditional server room or data centre models will not be sufficient in the longer term. An increasing number of services will be available only through the cloud and vendor support for on premise solutions is likely to diminish. Government must be in a position to adopt technologies such as blockchain, Artificial Intelligence and the Internet of Things to help re-invent how government services are delivered over the next few years and to support leading-edge ways of managing and analysing (large volumes of) data. In addition, the investment in national broadband will create new opportunities for digital access throughout the whole of Ireland.

A number of initiatives at national and international level may also impact the environment in which cloud services operate. These include for example:

The *Climate Action Plan 2019*[5] identifies the very rapid projected growth in electricity demand driven by technology, with data centres utilising as much as 31% of total consumption.

The Public Service reform plan, *Our Public Service 2020*[6], published in December 2017, states that the development of digital services and eGovernment is key to improving service delivery as is making better use of data and sharing data more effectively between organisations. It notes the drive towards a more integrated, shared and digital environment that will generate more efficiency and effectiveness in service delivery.

The *Public Service Data Strategy 2019 – 2023*[7] takes a whole-of-system approach to data management within the Public Service and the vision is to create a coherent ecosystem where public service organisations can confidently exchange data to support improved service delivery and policy creation. The target data ecosystem described in the strategy ensures that data exchange is performed in a legal, transparent and effective manner.

The *Data Sharing and Governance Act 2019*[8], which supports the Public Service Data Strategy, seeks to provide a legal basis to enable public service organisations, where they

[5] https://www.gov.ie/en/publication/ccb2e0-the-climate-action-plan-2019/
[6] https://ops2020.gov.ie/
[7] https://www.gov.ie/en/publication/1d6bc7-public-service-data-strategy-2019-2023/
[8] http://www.irishstatutebook.ie/eli/2019/act/5/enacted/en/html

already have a legal basis to collect data from the citizen or business directly, to collect that data from another public service organisation.

The *General Data Protection Regulation (GDPR)*[9] which took effect from 25 May 2018 has general application to the processing of personal data in the EU, setting out more extensive obligations on data controllers and processors, and providing strengthened protections for data subjects. Although the GDPR is directly applicable as a law in all Member States, it allows for certain issues to be given further effect in national law. In Ireland, the national law is the *Data Protection Act 2018*[10]. (In some circumstances previous Data Protection Acts still apply[11]).

Cloud computing, especially when architected to maximise efficient use of hardware and sharing of resources, provides opportunities to support these and other initiatives and to adapt to the challenges presented.

4. Vision

Government will ensure that the delivery and back-office systems underpinning knowledge management, policy development and the services provided to citizens and businesses, are run in the most secure and cost-efficient means possible. This will be achieved over time by migrating its systems, where practical, to government or public/mixed cloud environments.

In effect, this means that, at the macro level, public service organisations should take a “cloud-first” approach for all new systems and that Government systems should move to a hybrid-cloud environment, i.e. depending on data sensitivity, systems should migrate to either public cloud or government private cloud environments with connectivity established between these for the purposes of data sharing.

5. Principles

Research shows that organisations should no longer decide on *whether* to move to cloud for new or existing systems. The decision to be made now is *what, how* and *when* to move to cloud and which particular systems are suitable for cloud. If a system is deemed not suitable for public cloud a hybrid or private government cloud model should be considered. As public service organisations consider cloud options, the decisions reached to use or not use cloud

[9] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504
[10] http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html
[11] https://www.dataprotection.ie/en/legal/data-protection-legislation

for particular systems (with supporting reasons) should be documented and retained. Consequently, this advice note is based on three principles which are as follows:

5.1. ALL NEW SYSTEMS WILL BE DESIGNED TO MAXIMISE THE BENEFITS OF CLOUD

Organisations are required to identify if a cloud-based solution exists for all new systems under consideration. For off-the-shelf systems, organisations should review product roadmaps and engage with suppliers to identify if a cloud based solution exists. For bespoke systems, organisations should look at designing and building the system to maximise the benefits of cloud. In all cases, the decisions will be based on a number of considerations and the particular circumstances of the solution or organisation. A number of these considerations are set out at section 7.

5.2. ALL EXISTING SYSTEMS WILL BE REVIEWED REGULARLY FOR CLOUD CAPABILITY

Organisations should review, on a regular basis, all existing systems to, *inter alia*, assess which may be suitable for migration to the cloud. Priority should be given to systems where a major investment is being considered, for example implementing a new version or adding additional features. As with other decisions about their applications, the business owners are key contributors to the review process. Following a review, an organisation may decide that an existing system is not suitable for migration and instead retain and gradually retire the system[12]. However, where the decision made is to migrate an existing application, a number of options exist to achieve this. These range from re-hosting (some small modifications to move the application but taking no real advantage of cloud capabilities) to redesigning (with minor to major changes required to take some or greater advantage of cloud capabilities) to full replacement (designed for cloud).

5.3. A MOVE TO CLOUD WILL BE A BUSINESS DECISION ON THE BASIS OF SPECIFIC CONSIDERATIONS

To help focus a move to cloud, local multi-year cloud strategies should be developed which are linked to the organisation's overall strategy and which identify business outcomes to be achieved.

While taking a cloud-first approach, organisations should continue to assess their own requirements and seek the solutions that best enable them to achieve their business needs in a total cost of ownership value for money context. A cloud-first approach does not mean a cloud-only approach and financial, compliance,

[12] Although a UK Parliamentary Report on Digital Government (July 2019) suggested that "…'retain' should not be used widely as the proposed action in the long-term as there is clear evidence that the legacy system issue is going to increase over time and there are challenges with regard to the skills for supporting such systems." https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/1455/1455.pdf

technological, the risk profile of the data, and other issues may determine that cloud, in some/all of its variations, is not suitable for particular circumstances.

Some specific considerations are set out in section 7.

6. Delivery Models

Organisations will use cloud service models according to their specific requirements. Potential options for consideration include:

6.1. PRIVATE GOVERNMENT CLOUD

Private government cloud infrastructures are designed and configured for exclusive use by users from government organisations. Such infrastructure is owned, managed, and operated by (or on behalf of) government.

A private government cloud can exist on or off premise and is only accessible via Government Networks.

6.2. PUBLIC CLOUD

A public cloud infrastructure is designed and configured for open use by the general public and exists on the premises of the cloud provider. Public cloud providers offer standard, repeatable services at scale and on-demand. The main providers operate on a global basis and can meet large scale demand and requirements.

A public cloud exists off premise and is accessible via the public internet.

6.3. PUBLIC CLOUD OVER PRIVATE NETWORK

In this model, the public cloud infrastructure is used but accessed over a private network / dedicated communication link. The public cloud resources are interconnected to the internal resources of the organisation’s own datacentre.

A public cloud over private network exists off premise and is primarily only accessible via Government Networks.

6.4. HYBRID

Using cloud services is not an all-or-nothing decision. A hybrid approach, using services both from public cloud providers as well as an on premise Government managed private cloud, may be the appropriate approach for some systems. In such scenarios, organisations can split content and capability between the public cloud and the private Government cloud. This approach takes advantage of public cloud while addressing the considerations that make private government cloud more appropriate.

A hybrid can exist on or off premise and is accessible via Government Networks.

Organisations that have little or no experience with public cloud services should familiarise themselves with the various offerings by initially running a number of test or pilot projects, followed by projects with specific use cases in order to gain practical experience with real implementations[13]. This would require input from existing experts (for example from another public service organisation or externally). The pilots and specific projects should be implemented with more than one cloud provider to understand and compare the offerings available and to ensure that they support the range and depth of technologies an organisation requires. This will also help in evaluating the cost, benefits, shortcomings, as well as the work and skills required in developing new applications for or migrating existing applications to the cloud. Another key outcome should be an understanding of the impact on an organisation's security processes/controls. The pilots or specific projects should be run in the context of the considerations set out below and assessed on the basis of lessons learned rather than on success or failure.

7. Considerations

The decisions around moving to cloud will be based on a number of considerations. A selection of key considerations are set out below but there will be others specific to particular organisations and /or systems.

7.1. DATA CLASSIFICATION AND CATEGORISATION

A significant proportion of data processed by organisations, including personal data can be considered suitable for location in or migration to cloud services, subject to appropriate security controls and contract conditions being in place. In deciding what information can be put in the cloud and where (public, private, hybrid or not at all), organisations need to be able to identify the sensitivity of their data (including the impact of a data breach) and categorise it accordingly. This is not a trivial task but one which is required.

[13] Note that while pilot projects are useful, in themselves they may not bring out the full depth and breadth of impact across an organisation's systems environment.

While some organisations have a data classification system in place (for example the Department of Foreign Affairs and Trade), others do not and there are no central classification rules in place except for information defined as “top secret” - see Department of Finance *Circular 39/07 Classification of material as “top secret”*[14].

EU classified information (EUCI) is categorised in four levels: EU Top Secret, EU Secret, EU Confidential, and EU Restricted. These are set out in *Council Decision on the Security Rules for Protecting EU Classified Information*[15] and apply to the Council and its General Secretariat. They also need to be respected by public service organisations when they handle EUCI. The document has a mapping between the EUCI and equivalents across member states including Ireland.

Other data-related considerations include encryption, access rights, logging all access to data and managing data retention requirements.

7.2. PRODUCT

There are a number of issues to consider when choosing or using products built for or operating in the cloud.

Organisations need to review product roadmaps and engage with suppliers. In particular, for current products that are moving to a cloud only model, organisations need to ensure they understand the off-the-shelf features, functionalities, both core and configurable, as well as any relevant differences, update release cycles and the ongoing implications for bespoke customisations. This will help determine what cloud deployment models exist for the product, for example, some products may be moving to a SaaS-only model while others may not be available as SaaS.

Organisations also need to recognise the potentially transformative opportunities for business processes when adopting SaaS solutions and the impact that implementing customisations could have in the context of long term sustainability.

Organisations should review system workloads to identify peaks and troughs of utilisation and whether those are predictable or seasonal. This will be relevant in identifying if the systems can support auto-scaling which in turn may have implications for resources including costs.

Specific technical requirements may make cloud unsuitable (e.g. large scale online transaction processing (OLTP)) – organisations need to work with current on premise product providers to conduct a suitability analysis.

[14] https://assets.gov.ie/16354/836258897a554bb4ab9676aab0e31b17.pdf
[15] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013D0488

Organisations need to consider issues such as the resilience of the cloud offering and geo-separation, in particular in relation to business continuity / disaster recovery concerns.

Organisations need to balance the longer term inefficiencies (including costs) of migrating applications as they are into cloud environments against the costs of modernising in advance or replacing them altogether.

7.3. PUBLIC OR PRIVATE

In deciding on suitability for public or private cloud a balance needs to be struck between confidentiality, integrity and availability requirements. Information already in the public domain has no confidentiality requirements but may have very high availability requirements and would be a strong candidate for public cloud. In addition, public cloud infrastructures give access to new and enhanced functionality. For some solutions, the use of public cloud may be inevitable (e.g. no longer available on premise) and in that context, the decision here may be to ask whether private network access is required/ available.

Other considerations include obligations around data retention, National Archives requirements, and solution access requirements as well as the capacity and skills of organisations to properly use and manage the cloud service.

7.4. DATA-SHARING AND RE-USE

The *Public Service Data Strategy 2019 – 2023* aims at taking a whole-of-system approach to data management within the Public Service to create a coherent ecosystem where public service organisations can confidently and lawfully exchange data to support improved service delivery and policy creation.

The *Data Sharing and Governance Act 2019* seeks to provide a legal basis to enable government organisations where they already have a legal basis to collect data from the citizen or business directly, to collect that data from another government organisation.

In order to improve the various forms of data reuse across government organisations, a greater degree of standardisation in terms of systems, policies and practices is required. Organisations need to be aware of the above when considering using cloud based services and ensure their choices support and facilitate data-sharing and re-use.

7.5. DATA – PROCESSING VS STORAGE VS IN TRANSIT

For all systems but in particular when using cloud services, organisations must be aware of how their data is protected while being processed (in use), while stored (at rest) and while moving (in transit). The lifecycle of an information system must be closely managed to ensure that security concerns are proactively addressed at all stages. The approach to encryption at all stages is important here.

Organisations need to enhance their security practices in order to use cloud services in a way that enables them both to protect critical data and to make best use of the advantages that these services provide.

Organisations need to be clear on their data protection obligations but must also ensure that these obligations are not being used as a reason *not* to use cloud services without clear justification.

Data, including personal data, can be located in other EEA member states (EU plus Iceland, Liechtenstein and Norway). In considering location (including geo-separated locations), organisations will need to exercise due diligence on the offering and evaluate criteria such as track record and maturity. Organisations should also ensure that they can access their data in a way they want to for example through APIs (application programming interfaces). If real time checks are required, issues such as volumes and latency should be considered.

Other matters that need to be clear include: the responsibilities of the organisation for security versus those of the cloud provider for different “as a service” options; who is the data processor or the data controller in different circumstances?; who has access to the data at all stages?; what happens if there is a data breach?; where is the data stored (nationally, EEA, non-EEA)?; where are back-ups stored?; what is the audit capability (including third-party audit and activities such as penetration testing)? and who has access to the outcome?; encryption and key management – who is the custodian of the encryption keys?; etc.

7.6. TIMING

Given the complex nature of cloud projects, it takes time for an organisation to understand the various options and to put in place the in-house skills required to manage cloud services no matter how they are provided. An iterative approach is recommended with organisations improving their understanding and developing a range of processes (e.g. organisational, architectural, operations, governance) to manage their use of cloud services over time. The timescale to move to cloud also depends on the nature of the project. Proof of concepts, test projects or once-off projects versus key ongoing applications will have different timing requirements. In some circumstances specific urgent project deadlines may necessitate a cloud based solution or in others an on premise solution; these should be documented.

However, organisations need to develop a definite plan for new and existing systems with targeted deadlines.

7.7. GOVERNANCE

While cloud computing offers great opportunities for organisations it also presents a challenge to existing corporate risk and security management processes. These require special consideration to avoid unwanted exposure to risks in the area of costs and information security. Organisations should review and update their standards and processes where needed to reflect these challenges.

Issues to consider include adherence to (updated) standards and processes, clear division of responsibilities (within the organisation and between the organisation and the cloud service provider) including reporting and escalation processes, ensuring staff with the necessary level of cloud technological skills are available, configuration governance, usage management, access control, audit trails and access, data retention and archiving, as well as an exit strategy when changing provider.

Advice should be sought from Internal Audit on how good risk management of externally hosted systems can be demonstrated and objectively assessed.

Organisations that use cloud services from multiple cloud service providers need to ensure that they implement an organisation-wide approach to management and governance in their cloud environment. This includes standardising cloud policies and clarifying processes and ownership as well as considering for example using (or establishing) an internal brokering service to assist with the selection of the right services for end users. In also includes considering the use of a cloud access security broker (CASB) product or service.

7.8. CONTRACTUAL COVER

While recognising particular differences, as with other outsourcings decisions, organisations need to exercise strong due diligence in the selection of the cloud provider, the understanding and agreement of contract terms, and subsequent management of the service. Guidance should be sought from the Office of Government Procurement where necessary.

Key parts of the outsourcing decision include selecting a reputable cloud provider and ensuring service contracts cover any legal and regulatory obligations, location of data, security clearance of cloud provider staff, business continuity requirements and dispute resolution mechanisms.

Issues to consider include the licencing conditions, how costs are applied (given the elasticity of cloud services and pay-per-use models), service level agreements - including technical support and escalation procedures, back-up policies, and how upgrades occur.

Provider lock-in is largely inevitable and can occur at all cloud tiers, increasing from IaaS through PaaS to SaaS. Organisations should consider if a multi-cloud approach is appropriate to minimise any risk that may arise from provider lock-in. If selected, this approach should be factored into local practices to ensure they are properly governed. In addition, organisations need to develop a cloud exit strategy to manage issues such as poor cloud provider experience, cloud provider no longer offering the service, better offerings from another cloud provider, or the impact of regulatory requirements.

Organisations need to consider possible future requirements to move from the cloud provider and how, for example, data will be extracted in a useable form from the cloud provider and what happens to any copies held by them.

Organisations need to be clear as to the jurisdiction that will apply should any legal issues arise.

7.9. OTHER CONSIDERATIONS

Set out below are a number of other general factors which apply when considering new solutions and technologies. While some are touched on elsewhere in this advice note they are brought together here for convenience.

Procurement: Cloud computing, as with other ICT-related procurement, is subject to the requirements of Public Procurement. Given the specific nature of cloud services however, the Office of Government Procurement is planning to issue separate guidance in due course to complement this advice note.

Licencing: Organisations need to understand in detail the licencing model(s) for the products and avoid the overhead of unintended breaches of licence requirements. This will also be a factor in evaluating costs.

Costs: Close analysis and management of costs is required in a total cost of ownership value for money context. This includes understanding the difference between traditional on premise and cloud-based implementations, identifying initial costs as well as the ongoing (pay-as-you-go) usage costs, and, for example, managing the number and use of virtual machines, storage options, and the impact of “chatty” applications as well as the costs of supporting systems post migration.

Skills: Organisations need to ensure they have the relevant up-to-date skills in place to understand and manage a migration to (and from) cloud as well as to manage and support cloud based systems over their full lifecycle.

Technology stack: A move to cloud may impact on the overall technology stack used by an organisation. When assessing a cloud solution, organisations need to ensure they assess if particular products in their existing technology stack are supported or if alternative options are available.

Many of the considerations listed are not a point in time but a continuous process given the changing nature of cloud and the maturing nature of services offered. It is important that organisations keep abreast of the evolution of cloud services and the impact of new developments on existing and planned deployments.

8. Government Cloud

In line with the Build to Share stream of the Public Service ICT Strategy, the Office of the Government CIO delivers private Government Cloud services to public service organisations from Government Data Centres. The range and scale of services offered continues to expand and already includes compute and storage services i.e. IaaS. There is an ongoing programme to on-board organisations' systems to the private Government Cloud environment. This includes developing a strategy around implementation approaches to accelerate delivery of the private Government Cloud across the Public Service.

The private Government Cloud is supported by Government Networks which provides carrier-grade, high-capacity, resilient private telecommunications networks services to public service organisations nationwide.

The ambition for the Government Cloud is to provide wide functionality. However, given that these services are continuing to develop and expand, separate information on the services will be issued as they become available.

9. Other Matters

9.1. DATA PROTECTION

The Data Protection Commission has prepared guidance[16] to assist organisations understand their obligations with regard to the security of personal data, and to mitigate their risks when utilising a cloud-based environment. The DPC advises that

[16] https://dataprotection.ie/en/guidance-landing/five-steps-secure-cloud-based-environments

organisations should determine and implement a documented policy and apply the appropriate technical security and organisational measures to secure any cloud-based environments they utilise.

The Data Protection Commission also provides guidance on transfers of personal data to third countries or international organisations[17]. The guidance includes information on transfers on the basis of an "adequacy decision"; transfers subject to appropriate safeguards (including standard data protection clauses); as well as derogations for specific situations.

The European Data Protection Board[18] (EDPB) issued *Guidelines on the use of cloud computing services by the European institutions and bodies*[19] in March 2018. The guidelines while aimed at the Data Protection Officers, Data Protection Controllers, ICT and other services of EU institutions, may be a useful reference to other public service organisations, although some specific details are particular to EU institutions.

The EDPB has issued draft guidelines on the territorial scope of the General Data Protection Regulation[20]. The draft guidelines "seek to ensure a consistent application of the GDPR when assessing whether particular processing by a controller or a processor falls within the scope of the GDPR". They set out and clarify "the criteria for determining the application of the territorial scope of the GDPR".

9.2. CERTIFICATION

An organisation may look at a cloud service provider's compliance with certification schemes to seek assurance in relation to the cloud service provider itself and in relation to the individual services it offers. There is no single relevant certification scheme for cloud computing and an EU study from 2018, *Certification Schemes for Cloud Computing*[21], found that compliance with existing certification schemes is a big challenge for cloud service providers. This is mainly due to the high market fragmentation of cloud and security certification schemes. The study analyses six certification schemes in depth, with the aim of comparing the key areas on which each focuses, such as procurement management, operational security, and security integrity. It found that ISO 27001 is currently the most adopted certification scheme

[17] https://www.dataprotection.ie/en/organisations/international-transfers

[18] https://edpb.europa.eu/edpb_en

[19] https://edps.europa.eu/data-protection/our-work/publications/guidelines/guidelines-use-cloud-computing-services-european_en

[20] https://edpb.europa.eu/our-work-tools/public-consultations/2018/guidelines-32018-territorial-scope-gdpr-article-3_en

[21] https://ec.europa.eu/digital-single-market/en/news/regulating-cloud-computing-europe-new-study-considers-options-certification-schemes

by the 50 cloud service providers it analysed. Other relevant schemes following ISO 27001 include CSA Star, PCI-DSS and the SOC series.

The European Union Agency for Network and Information Security (ENISA) gives an overview of different existing certification schemes[22] which could be relevant for cloud computing customers. ENISA provides an online tool[23] that allows customers to choose a set of relevant security objectives and to see which of these security objectives are addressed by various cloud certification schemes. The EU study (above) maps the ENISA security objectives against a wide range of certification schemes, standards and best practices.

10. Additional Supporting Material

Given the continued rapid developments in cloud computing it may be necessary to issue additional supporting documents over time rather than wait for a revision of this advice note.

11. Summary

Subject to a business decision on the basis of specific considerations, all new government systems should be developed to exploit the opportunities presented by cloud deployment, where possible, and all existing systems will be reviewed for cloud capability. This will happen over time and where practicable.

This advice note aims to provide high-level guidance to assist public service organisations in making decisions in relation to the adoption of cloud services. The information provided is not intended to be exhaustive and if required organisations should seek further advice from organisations or providers with recognised relevant experience.

While recognising that a cloud-first approach does not mean a cloud-only approach, a move to cloud services of whatever type is inevitable for many applications or solutions whether by choice of the organisation or enforced by solution providers. On that basis, organisations should now be developing their own cloud strategy and specific cloud management policies. Plans should include identifying and prioritising applications that are suitable for cloud deployment or migration and should set specific timelines to achieve this.

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

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

Tithe an Rialtas, Sráid Mhuirfean Uacht
Baile Átha Cliath 2, D02 R583, Éire

Government Buildings, Upper Merrion Street
Dublin 2, D02 R583, Ireland

T +353 1 676 7571

@IRLDeptPer

www.gov.ie/per