NSAI Standards

SWiFT 10:2012

Adopting the Cloud - decision support for cloud computing

SWiFT 10:2012

Incorporating amendments/corrigenda/National Annexes issued since publication:

The National Standards Authority of Ireland (NSAI) produces the following categories of formal documents:

I.S. xxx: Irish Standard – national specification based on the consensus of an expert panel and subject to public consultation.

S.R. xxx: Standard Recommendation - recommendation based on the consensus of an expert panel and subject to public consultation.

SWiFT xxx: A rapidly developed recommendatory document based on the consensus of the participants of an NSAI workshop.

This document replaces:	*This document is based on:* SWiFT 10:2012	*Published:* 4 April, 2012

This document was published under the authority of the NSAI and comes into effect on: 4 April, 2012	ICS number: 35.110 35.240

NSAI
1 Swift Square,
Northwood, Santry
Dublin 9

T +353 1 807 3800
F +353 1 807 3838
E standards@nsai.ie
W NSAI.ie

Sales:
T +353 1 857 6730
F +353 1 857 6729
W standards.ie

Údarás um Chaighdeáin Náisiúnta na hÉireann

Contents

Page

Acknowledgement

NSAI would like to acknowledge input of the Irish Internet Association (IIA) Cloud Computing Working Group in the development of this SWiFT, and the work of ISO/IEC JTC 1 SC 38 final report of the Study Group Report on Cloud Computing. In particular NSAI wishes to acknowledge the work of Lavinia Morris (Friends First) who chaired the working group and Joan Mulvihill the CEO of the IIA for steering the work of the project.

The Irish Internet Association is the trade association for all internet businesses in Ireland. The association which has been in existence since 1997 is tasked with connecting businesses, promoting online business, providing knowledge and expertise for all companies looking to engage with online services or selling. Members range from the largest multi-national corporations to independent developers, start-ups and SME consumers of technology.

The IIA Cloud Computing Working Group is a collaboration of expert practitioners and business leaders (Chief Information Officers, Chief Technical Officers, Heads of IT, Legal, Consultancy) from a variety of business sectors and organization sizes in Ireland. The group, which has equal representation from both the Cloud vendor and Cloud customer communities, seeks to educate decision makers with a balanced view of the advantages, challenges, opportunities and limitations of Cloud Computing.

Foreword

This document SWIFT – **S**tandardized **W**ithin the **F**ast **T**rack (process) was developed based on the consensus of the individuals listed below all of whom are members of the IIA Cloud Computing WG.

Lavinia Morris	Friends First
Joan Mulvihill	Irish Internet Association
Trevor Dagg	Talentevo
Niall Moran	Lucey Technology
Peter O'Neill	Mason Hayes & Curran
Pearse Ryan	Arthur Cox
Gerry Power	Sysco
Padraig Sugrue	Accenture
Mark Greville	Bank of America Merrill Lynch
Brona Kernan	Irish Times
Jared Carstensen	Deloitte
Wilbour Craddock	Microsoft
Keith Eccles	Oracle
Stephen Moffatt	IBM
Cian Blackwell	Grant Thornton
Sean Hickey	H&K International
Noel Comerford	ESB

Introduction

Cloud computing is undoubtedly one of the most widely discussed innovations of the last few years. Both national and international growth predictions are staggering and as a result every organization is asking itself, whether it should be considering Cloud computing.

Cloud computing, however, covers such a wide variety of information technology (IT) from the relatively simple to the extremely complex that many people find the term confusing. It is not surprising, therefore, that when organizations seek to use Cloud computing there are many questions to consider and it is not always clear where to start.

The IIA Cloud Computing Working Group in conjunction with the National Standards Authority of Ireland have devised a Decision Support Matrix designed to provide guidance to organizations both large and small on the various items that need to be considered when adopting Cloud computing. When considering Cloud adoption it is important for organizations to be fully informed of both the risks and benefits. These will vary from business to business and from application to application as no two organizations are alike.

This SWiFT serves to provide a generic series of questions across a broad range of categories. It is not intended to be an exhaustive examination of this rapidly evolving area but rather a guide based on the experiences of the Working Group to date. Not every question will be relevant to every deployment and what presents a challenge for one organization could be a benefit for another depending on the nature of the deployment, the application being considered and the organization in question.

What is Cloud computing?

There have been many official definitions of Cloud computing developed over the past number of years. The definition of Cloud computing that underpins this SWiFT is that from National Institute of Standards and Technology and ISO/IEC JTC 1 (see Figure 1). Full details of this definition can be found in Annex A of this guide. Annex B provides a useful summary of Cloud computing initiatives taken from the ISO/IEC JTC 1/SC 38 Study Group Report on Cloud Computing.

At a basic level Cloud computing is about using computing services based in the internet (or the Cloud) rather hosting them locally. In reality many people are already using Cloud computing in everyday life without even realizing it. Services such as e-mail, social networking, photo sharing, etc. are all forms of Cloud computing. From a business perspective Cloud computing is essentially an evolution of managed services and outsource arrangements that have been available for many years.

In a general sense Cloud computing can be divided into three delivery models, four deployment models and five essential characteristics as described below. The characteristics of each are quite different and therefore it is important to understand them when considering Cloud computing.

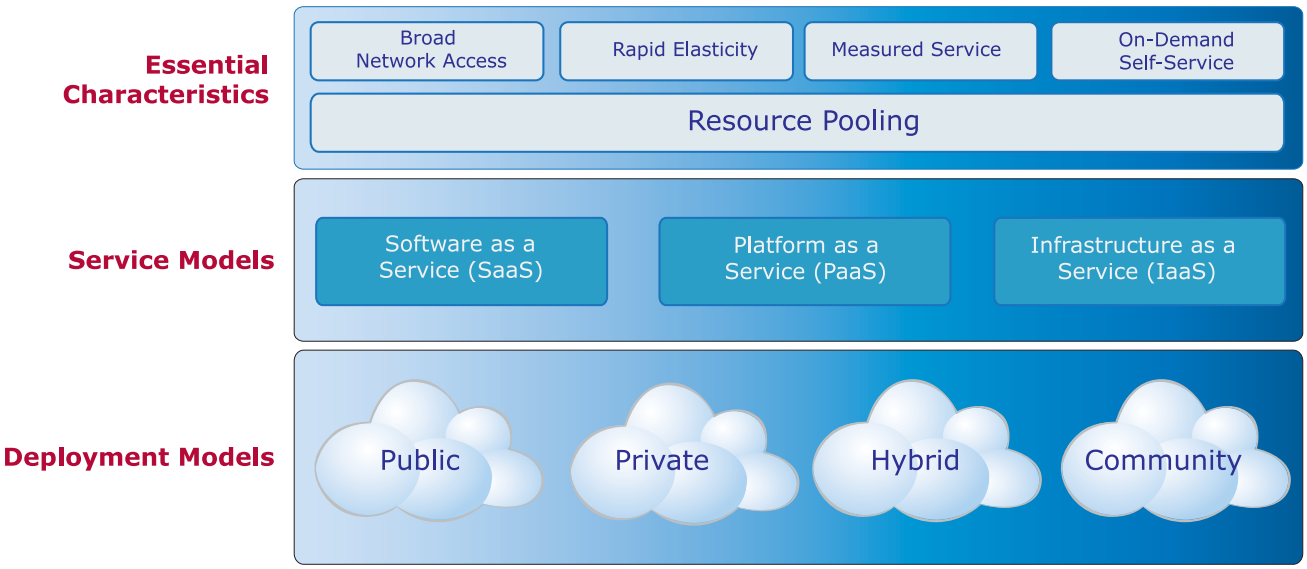

Figure 1 — NIST definition of Cloud Computing

Delivery models:

1) *Infrastructure as a Service (IaaS):* as the name suggests this is essentially the provision of infrastructure services or piping and plumbing (e.g. servers, storage, network, etc.) in the Cloud.

2) *Platform as a Service (PaaS):* under this model, as well as providing the underlying piping and plumbing the vendor also provides the application development platform for development of applications.

3) *Software as a Service (SaaS):* probably the most well-known version of Cloud Computing; under this model the vendor provides the entire suite of services from the underlying piping and plumbing to the application itself.

Essential characteristics:

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

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

3) *Resource pooling.* The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

4) *Rapid elasticity.* Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand.

5) *Measured service*. Cloud systems automatically control and optimize resource use by leveraging a metering capability[1] at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts).

Deployment models:

1) *Private Cloud.* The Cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

2) *Community Cloud.* The Cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organization or a third party and may exist on premise or off premise.

3) *Public Cloud.* The Cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling Cloud services.

4) *Hybrid Cloud.* The Cloud infrastructure is a composition of two or more Clouds (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).

Intended user of this SWiFT Document

SWiFT 10 has been developed for use by businesses of all sizes considering the adoption of Cloud Computing. Ultimately the decision to adopt Cloud Computing is a strategic technology decision and therefore it is important that all relevant parties are engaged in this analysis. Every effort has been made to make the guide as straightforward as possible but some technical input will be required in certain areas. For large organizations with dedicated IT departments we recommend the guide be completed by the CTO in conjunction with the appropriate representatives from other areas of the organization such as legal, compliance, operations, finance, etc. For smaller organizations we recommend the guide be completed by the CEO with input from a trusted IT supplier or a 3rd party expert practitioner in the area of Cloud Computing.

Disclaimer

This document is intended to support businesses and organizations of all types in making decisions on the adoption of Cloud technologies. It is a general guide intended to cover a wide range of circumstances, and cannot reflect all of the particular requirements of every organization. Ultimately, any decisions on the adoption of business technology should be made by users based on their own judgement, supported by professional advice where required. Neither the authors nor the publishers of this document can accept liability for any loss incurred by any person acting or refraining from acting on as a result of material in this document.

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

Adopting the Cloud – decision support for Cloud computing

1 Scope

This SWiFT has been compiled as a generic guide to encompass all Cloud delivery models and deployment models. It is intended for use as a means of assessing Cloud adoption suitability and should be used in conjunction with available reference models for a deeper analysis.

2 Terms and Definitions

For the purpose of this document the following terms and definitions apply. These definitions are not necessarily identical to the ISO/IEC definitions.

bandwidth
rate of data transferred in or out of a network

NOTE Usually measured in bits per second

data centre
facility used to house computer systems and associated components, such as telecommunications and storage systems.

NOTE It can be customer owned or supplier owned

data controller
person who, either alone or with others, controls the contents and use of personal data, as specifically defined in the Data Protection Acts (DPA)

data processor
person who processes personal data on behalf of a data controller but does not include an employee of a data controller who processes such data in the course of his employment, as specifically defined in the DPA

eDiscovery
any process by which electronic data are sought, located, secured, and searched with the intent of using them as evidence in a civil or criminal legal case

escrow
source code and documentation that is kept in the custody of a third party until specified contractual conditions have been fulfilled

[SOURCE: ISO/IEC 26514:2008]

multi-tenancy
provision of the same implementation of a system to multiple customers (tenants)

on-premise
infrastructure, software and/or IT services installed and running in the building or data centre of the person or organization using them

open-source
software development whereby the code is freely available

NOTE The resulting software is then normally provided to customers free of charge although enterprise support agreements are available in some cases.

segregation of duties
separation of functions within a software system to different locations so that they can be secured independently and operate in isolation

thick client
application that is installed locally on a client device and uses the graphic, storage and processing capabilities of the device

NOTE Client devices can include PCs, laptop smart phones etc.

uptime
measure of the time the service is expected to be available to a business in an agreed time period

NOTE Usually expressed as a percentage, e.g. 99.95%

personal data
information relating to an identified or identifiable individual that is recorded in any form, including electronically or on paper

[SOURCE: ISO/IEC TR 24714-1:2008]

service credit
commercial arrangement whereby the supplier of services either has reduced from recurring charges, or provides a customer with a form of credit against recurring charges in circumstances where the supplier fails to achieve service levels over an agreed measurement period

NOTE Generally represented as a percentage of the overall recurring charge.

virtual machine
a virtual data processing system that appears to be at the exclusive disposal of a particular user, but whose functions are accomplished by sharing the resources of a real data processing system.

[SOURCE: ISO/IEC 2382-1:1993]

3 Symbols and abbreviations

Capex
Capital expenditure
expenditure that is upfront and once off

CTO
Chief Technical Officer

DPA
Data Protection Acts 1988 and 2003

IDS
Intrusion Detection System
technical system that is used to identify that an intrusion has been attempted, is occurring or has occurred, and possibly to respond to intrusions in IT systems and networks

[SOURCE: ISO/IEC 18028-3:2005]

DLP
Data Loss Prevention
process of preventing data from being compromised

Opex
Operational expenditure
expenditure that is ongoing

PCI
Payment Card Industry
certification required by any data processor that processes credit card details in any way

CAIQ
Consensus Assessments Initiative Questionnaire

NOTE This is compiled by the Cloud Security Alliance.

SLA
Service Level Agreement
agreement on the nature and quality of service between a consumer and a service provider

4 Completing the Cloud Adoption Decision Support Matrix

Drawing on the experience of the IIA Cloud Computing Working Group the Decision Support Matrix has been divided into a number of categories which have proved either challenging or beneficial to businesses considering the adoption of Cloud Computing. Under each category a series of questions are posed which are designed to provoke thought and discussion. When answering the questions organizations are advised to consider both the risk and the benefit for their business - a simple High(H), Medium(M), Low(L) scale is used to capture this at a high level. (An organization's own risk management regime could equally be used in conjunction with the questions provided in this matrix). Using the guide in this way will allow organizations quickly to assess the benefits and challenges of Cloud Computing and hence the overall suitability.

5 The Cloud Adoption Decision Support Matrix

5.1 Context

The first step in completing this guide is to assess why Cloud Computing is being considered for the organization and its impacts.

Question/Consideration	Answer	Risk (H/M/L)	Benefit (H/M/L)
1. What are the key benefits which are expected from the use of Cloud?			
2. What impact will adoption of Cloud have on end users of the organization?			
3. Will the use of Cloud allow the achievement of objectives not possible by other means?			

5.2 Nature of deployment

The next step is to consider the nature of the service or application under consideration for Cloud adoption and its suitability for the Cloud model.

Question/Consideration	Answer	Risk (H/M/L)	Benefit (H/M/L)
1. Is it planned to deploy a new application or service to the Cloud or migrate an existing application or service?			
2. Will adoption of Cloud technology enable quicker time to market than an on-premise deployment?			
3. a) What is the typical application or service use - predictable, unpredictable, seasonal, unknown?			
b) Will it benefit from the flexibility of the Cloud model?			

5.3 Security

Security is undoubtedly one of the key considerations for Cloud adoption and indeed is regularly cited as one of the main inhibitors to Cloud adoption. The level to which it may become an inhibitor depends on the nature of the service an organization is planning to operate in the Cloud, the model of Cloud in which it is deployed and the maturity of an organization's own security policy. The list below is not intended to be exhaustive and should be used in conjunction with one of the established security questionnaires (e.g. Cloud Security Alliance (CSA) CAIQ, ISO/IEC 27000 series) as part of thorough due diligence.

Question/Consideration	Answer	Risk (H/M/L)	Benefit (H/M/L)
1. What physical access control requirements are required and how are these satisfied by the Cloud provider (e.g. entry to data centres, access to servers)?			

Question/Consideration	Answer	Risk (H/M/L)	Benefit (H/M/L)
2. What logical access control requirements are required and how are these satisfied by the Cloud provider (e.g. administrative accounts, access to virtual machines, data, etc.)?			
3. What monitoring and alerting processes are required and how are these satisfied by the Cloud provider (e.g. IDS, DLP, segregation of duties, etc)?			
4. What data confidentiality protection processes are required and are these satisfied by the Cloud provider (e.g. encryption)?			
5. What data continuity verification processes are in place (e.g. how are data backed up, are data removed from impaired disks, etc.) and are these satisfied by the Cloud provider?			
6. What level of data segregation is provided and what controls are in place around this segregation?			
7. a) What level of logging and auditing is required?			
b) What level of access to audit log data can the Cloud vendor provide?			
c) What protection and assurance over audit log data (e.g. encryption, evidence of tampering, backups, etc.) are in place?			
8. How long can log data be retained?			
9. Are salvage rights to data, code or configurations associated with the Cloud solution required and if so is escrow applicable?			
10. a) Is eDiscovery relevant to the data under the control of the Cloud provider?			
b) If so, does the Cloud provider deal with litigation assistance in the contract or supporting corporate policy documents?			
c) Has the Cloud provider any experience of litigation assistance and is such assistance provided on a chargeable or non-chargeable basis, including details of charges?			
11. a) Is compliance with PCI, ISO/IEC 27001 or other international security standards required?			
b) Are there industry specific security standards to which you must adhere?			
c) If so, does the Cloud provider comply with all relevant standards?			

Question/Consideration	Answer	Risk (H/M/L)	Benefit (H/M/L)
d) What level of due diligence can be conducted to verify compliance with these standards?			
12. a) What breach notification policies are in place in any case where supplier security has been compromised (even if that compromise does not immediately indicate a compromise to the services/ data hosted for the organization)?			
b) What supplier breach notification policies are in place for a breach in security that directly relates to the systems, services or data of the consumer of the Cloud service?			
13. Has the Cloud provider subcontracted any of the services to third parties or is the Cloud provider using the services of a third party in the provision of the service (e.g. PaaS, IaaS) and if so are there adequate controls in place?			

5.4 Data privacy and protection

One of the key advantages of Cloud computing is its global nature; however, exporting personal data outside of the European Economic Area is very heavily regulated. Consequently, any organization considering adoption of Cloud computing needs to be fully aware of its obligations under all applicable data protection legislation and to ensure that all necessary safeguards are in place.

NOTE The DPA lays down provisions in this regard.

Question/Consideration	Answer	Risk (H/M/L)	Benefit (H/M/L)
1. a) What data are to be put in the Cloud?			
2. b) Are they sensitive data (e.g. health data or financial data) where the consequences of a data breach could be serious?[2]			
3. Which national and international data protection, security or privacy laws apply to the data processed by the Cloud provider (e.g. DPA, the Patriot Act, Safe Harbor, etc)?			
4. Has it been determined whether under applicable data protection legislation:			
a) the organization is a data controller or data processor			
b) the Cloud provider is a data controller or data processor			

[2] The DPA has specific provisions dealing with 'sensitive personal data.' The Office of the Data Protection Commissioner has also published a Code of Practice for managing data breaches, which should be complied with in the event of a data breach.

Question/Consideration	Answer	Risk (H/M/L)	Benefit (H/M/L)
c) the Cloud provider has sufficient security measures in place to protect personal data			
5. a) Where is the Cloud provider's data centre(s) (to be used in the provision of this service) based? Is it within or outside the EEA?			
b) If outside the EEA, have international data transfer issues been considered?			
6. a) Can the Cloud provider guarantee where the data will be stored?			
b) Does the Cloud provider subcontract any of the services provided (including any SaaS supplier use of third party PaaS or IaaS services)?			
7. a) Is it necessary to tell customers or employees that their data are moving to the Cloud?			
b) Do existing data protection consents or notices cover the transfer?			
8. a) Does the Cloud provider contract contain a data protection clause?			
b) If so, is it compliant with applicable data protection legislation?			
9. Does the supplier have a policy around disclosure regarding data breaches above and beyond local European and international data protection legislation?			

5.5 System availability

As Cloud computing changes the model by which computing services are deployed it is important to consider and understand the impact, both positive and negative, that it will have on system availability. The criticality of this impact will vary depending on the business criticality of the application or service being considered for Cloud deployment.

Question/Consideration	Answer	Risk (H/M/L)	Benefit (H/M/L)
1. What are customer uptime expectations?			
2. What are the financial and/or liability management implications of a service outage?			
3. What are the reputational implications of a service outage?			
4. a) Are there any availability SLAs that must be adhered to?			
b) How does the Cloud provider's availability SLAs compare to current on-premise SLA achievement?			
5. a) Are there any performance SLAs that must adhered to e.g. transaction speed?			

Question/Consideration	Answer	Risk (H/M/L)	Benefit (H/M/L)
b) How does the Cloud provider's performance SLAs compare to current on-premise SLA achievement?			
6. How many system outages and, if any, of what type or extent has the Cloud provider had in the past six months and is this within acceptable risk tolerances?			
7. Does the Cloud provider provide SLAs which are appropriate and of sufficient detail to meet the needs of the organization?			
8. Is it exactly understood how the SLAs are measured by the Cloud provider?			
9. a) Does a service management regime support the service levels, including a service reporting, remedial planning and service credit regime?			
b) Does the service credit regime provide reasonable compensation in circumstances of failure to achieve service levels?			
10. a) Are service credits expressed on a sole remedy or sole liability basis or other form of reference to the contract liability exclusion or limitation provisions?			
b) Are the consequences of such references understood?			

5.6 Network infrastructure

Under the Cloud computing model the network infrastructure providing internet access is critically important. Ensuring it is sized correctly as well as being suitably reliable and having sufficient inbuilt redundancy is critical for a successful Cloud deployment.

Question/Consideration	Answer	Risk (H/M/L)	Benefit (H/M/L)
1. How performant and reliable is the internet infrastructure required to support the Cloud solution?			
2. What is the bandwidth requirement for communication between existing on-premise solutions and the Cloud solution being considered?			
3. Will an upgrade to the existing infrastructure be required to accommodate this?			
4. What latency is required for communication between on-premise solutions and the Cloud solution being considered; can this be accommodated?			

5.7 Flexibility

One of the key benefits of Cloud computing is the deployment flexibility it offers organizations.

Question/Consideration	Answer	Risk (H/M/L)	Benefit (H/M/L)
1. How important is application or service portability?			
2. Will moving to the Cloud improve the portability of the application or service?			
3. Can the application or service be transitioned back on-premise from the Cloud or is it a Cloud only application or service?			
4. Can the application or service be transitioned to another Cloud or is it vendor specific?			
5. To what level will moving to the Cloud change the control which the organization has over the application or service being considered for transition?			
6. Can existing software licences be transitioned to the Cloud solution in a case where existing application(s) or service(s) are being migrated?			
7. In the event that the application or service is to be migrated from the Cloud back on-premise, can the Cloud software licences be transitioned accordingly?			
8. What are the cost implications associated with the above licence transition scenarios?			

5.8 Data storage and extraction

Data are the core asset of most organizations and therefore it is important to understand how the data will be managed under any proposed Cloud model. Data retention, backup, growth and extraction should all be considered and planned for in advance.

Question/Consideration	Answer	Risk (H/M/L)	Benefit (H/M/L)
1. Will the Cloud be the primary data store for the application or service?			
2. Does the Cloud service provider offer data backup, replication and recovery options?			
3. Does the Cloud provider offer SLAs with respect to each of the above options and how do they compare against the organization's SLAs?			
4. Does the Cloud provider offer an ability to take the data out of the Cloud service and if so at what cost?			

Question/Consideration	Answer	Risk (H/M/L)	Benefit (H/M/L)
5. a) How much data is it foreseen the Cloud service will need to support?			
b) Would it be physically possible to transition the data to another provider or back on-premise if required?			
c) How would the data transition be achieved in the above transition scenarios?			
d) Are there formatting, structure or other technical obstacles to data transition?			
6. a) Does the Cloud provider offer a standard exit route, including timelines for the business to transition to another Cloud provider or back on-premise?			
b) Are there reference sites available where an exit route, where offered, has been successfully followed?			
7. Are the data maintained in its correct format (e.g. encrypted) and will all the necessary components required to access the data be available (e.g. keys)?			
8. a) What are the backup retention requirements?			
b) Can the Cloud provider meet these requirements?			
9. Is the appropriate level of access which is required to meet the needs of the organization available to data stored in the Cloud?			

5.9 Capacity Planning

Consideration should be given to the expected growth of the application or service and the extent to which this favours or impacts upon a Cloud adoption model.

Question/Consideration	Answer	Risk (H/M/L)	Benefit (H/M/L)
1. What is the expected growth rate over the next five years?			
2. What will be the impact of this growth if the application or service is accommodated on-premise?			
3. What will be the impact of this growth if the application or service is accommodated in the Cloud?			

Question/Consideration	Answer	Risk (H/M/L)	Benefit (H/M/L)
4. Is the application or service time bound (e.g. batch processing)?			
5. How does the Cloud provider manage capacity increase requirements and is this dealt with contractually?			
6. Have each of the above been considered in the context of a capacity decrease?			

5.10 Customizations

Consideration should be given to the level of customization required, if any, and the extent to which this favours or impacts upon a Cloud adoption model.

Question/Consideration	Answer	Risk (H/M/L)	Benefit (H/M/L)
1. Is the application or service heavily integrated with other applications?			
2. If so, where are these applications or services accommodated – on-premise, same Cloud provider, different Cloud provider or other?			
3. For applications which are integrated with other on-premise applications, is real-time interaction with the Cloud database required? (e.g. handheld integration). If so, what real-time integration technologies need to be considered?			
4. Has it been confirmed that the application language is compatible with the Cloud solution under consideration?			
5. Is the application or service customized for the needs of the organization or is it an 'out of the box' solution?			
6. Are there restrictions due to multi-tenancy of the Cloud infrastructure on what can or cannot be customized?			
7. Does the application or service require special hardware to operate on-premise that might act as an obstacle to moving it to Cloud (e.g. a mainframe)?			
8. Is the application or service based on commercial or open-source software?			
9. If the application or service is based on commercial software, what are the licensing implications of moving to the Cloud?			
10. Are there any reference applications or services with similar levels of customization and integration which demonstrate the feasibility of the Cloud?			

Question/Consideration	Answer	Risk (H/M/L)	Benefit (H/M/L)
11. What type of client will be used to access the application or service (mobile, web, thick client) and will the use of Cloud help or hinder this?			

5.11 Maturity and adoption

Cloud computing is still an emerging phenomenon with many new vendors and offerings entering the market. It is important to understand the maturity and adoption rate of any Cloud vendor or application or service being considered.

Question/Consideration	Answer	Risk (H/M/L)	Benefit (H/M/L)
1. How well established is the Cloud vendor being considered?			
2. How mature is the Cloud vendor and what are the current levels of adoption?			
3. Is the product roadmap available and if so is it satisfactory?			
4. a) Has the Cloud provider provided satisfactory information in relation to numbers of existing clients?			
b) Are the existing clients available as 'reference' sites?			

5.12 Contingency planning

Contingency planning is vital particularly in circumstances where all systems control has been handed over to a Cloud provider. It is important to understand the contingency arrangements in place and the breakdown of responsibility for these arrangements.

Question/Consideration	Answer	Risk (H/M/L)	Benefit (H/M/L)
1. a) Does the Cloud provider operate documented contingency and disaster recovery policies and procedures in relation to its services?			
b) Are these acceptable to the organization?			
2. In particular, does the Cloud provider operate an acceptable policy in circumstances of data centre failure?			
3. What is the breakdown of contingency responsibilities between the organization and the Cloud provider?			

Question/Consideration	Answer	Risk (H/M/L)	Benefit (H/M/L)
4. Has this been considered from a risk management perspective, including contractually?			

5.13 Internal skill-sets and governance

Organizations need to anticipate the impact Cloud computing will have on the IT department. Job roles, processes and governance model implications all need to be considered when adopting the Cloud.

Question/Consideration	Answer	Risk (H/M/L)	Benefit (H/M/L)
1. Will the Cloud allow the IT team to work more efficiently and if so how?			
2. What level of IT organizational change will be needed?			
3. a) What skill-set changes will be required?			
b) Will new internal skill-sets be required to support and extend the application or service?			
c) What internal skill-sets can be retired?			
d) What existing internal IT roles will need to evolve to accommodate Cloud adoption?			
4. What level of IT administration will need to be retained and what level of IT administration can be transitioned to the Cloud provider?			
5. What level of training for internal staff will be required to support and extend the application or service?			
6. a) What changes to process and procedure will be required?			
b) In particular what changes will be required in service management processes to support the introduction of Cloud?			
7. Will a Cloud based application or service be easier or more difficult to support and maintain?			

5.14 Commercial considerations

When considering the commercial implications of adopting Cloud computing it is important to understand the overall cost and not just the headline figures. A thorough assessment and understanding of all the commercial implications are recommended.

Question/Consideration	Answer	Risk (H/M/L)	Benefit (H/M/L)
1. How does the Opex versus the Capex cost compare over a defined period of time e.g. a five-year period (including maintenance and upgrade costs)?			
2. Are there additional costs that need to be considered outside the headline per month figures e.g. additional security and audit costs, data transfer costs, staff training costs, etc.?			
3. a) Is the Cloud provider pricing model understood clearly?			
b) In particular, is the pricing model stationary or managed-variable, or can price be varied by Cloud provider notice?			
c) Are there any data or user maxima ('caps') that apply to the offering (e.g. quantity of users, size of data)?			
d) Are the commercial implications of both an increase and decrease in capacity understood?			
4. a) What level of IT administration will need to be retained and what level of IT administration can be transitioned to the Cloud provider?			
b) Will new administration skill-sets be required?			
c) How will this translate in terms of on-premise staff costs or savings?			
5. a) Is the Cloud provider considered financially secure?			
b) Has a review of the Cloud provider's published accounts over a period that is considered necessary by your organization been carried out and are the results satisfactory?			
c) Have the circumstances of the possible insolvency of the Cloud provider and/or its sub-providers been considered?			
d) Does the Cloud provider offer an escrow arrangement or other arrangement of assistance in such circumstances and is it workable in practice?			

Question/Consideration	Answer	Risk (H/M/L)	Benefit (H/M/L)
6. Is the shareholding of the Cloud provider, including percentage of shareholding held by venture capitalists and any noteworthy shareholder lock-in periods, understood?			
7. a) Have insurance issues generally applicable to a Cloud computing transaction been considered and, in particular, have issues associated with cyber or data risk been considered?			
b) Are the insurance policies of the Cloud provider and the organization considered adequate given the nature of the loss or damage which could be suffered as a result of Cloud provider default?			
c) Where necessary, have the organization's insurers been notified of the proposed Cloud contract?			

5.15 Cloud contracts

Cloud computing involves the remote provision of computing service, which is a commercial arrangement between a customer and a supplier based on a contract. The Cloud contract controls the relationship between the parties and is of central importance to any Cloud computing transaction or project.

Question/Consideration	Answer	Risk (H/M/L)	Benefit (H/M/L)
1. a) Does the Cloud provider operate a standard contract?			
b) If so, is the Cloud provider willing to negotiate this standard contract?			
c) If not, is the Cloud provider willing to contract on the basis of the contracting organization's standard contract?			
2. What guarantees (if any) around service provision are included in the Cloud contract (e.g. Availability SLAs, Performance SLAs, etc.) or does the Cloud contract exclude all guarantees or legal warranties?			
3. a) What exit path is provided for in the contract?			
b) Are the terms of such exit path, if any, extensive enough to meet the requirements of the organization?			
4. In the event of litigation, what level of support to the organization by the Cloud provider is provided for in the contract?			
5. a) What governing law and dispute resolution forum apply in the Cloud contract and are these			

Question/Consideration	Answer	Risk (H/M/L)	Benefit (H/M/L)
considered acceptable?			
b) Is this arrangement regarded an effective route to remedy against the Cloud provider in circumstances of Cloud provider default?			
6. Does the organization regard the contract liability management provisions, including any exclusion and limitation of Cloud provider liability, as providing an effective remedy against the Cloud provider in circumstances of Cloud provider default?			
7. Does the organization regard the Cloud provider contract as reflecting a reasonable or unreasonable allocation of risk between customer and supplier? (In this regard see Section 5.14 in relation to insurance matters.)			

Annex A
(informative)

Definition of Cloud Computing
(based on NIST Special Publication 800-145)

A.1 Definition of Cloud computing

A.1.1 General

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.

A.1.2 Essential characteristics:

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

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

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

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

5) *Measured service*. Cloud systems automatically control and optimize resource use by leveraging a metering capability[3] 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.

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

A.1.3 Service Models:

1) *Software as a Service (SaaS).* The capability provided to the consumer is to use the provider's applications running on a Cloud infrastructure[4]. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based e-mail), or a program interface. The consumer does not manage or control the underlying Cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

2) *Platform as a Service (PaaS).* The capability provided to the consumer is to deploy onto the Cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider[5] 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.

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

A.1.4 Deployment Models:

1) *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.

2) *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.

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

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

---

[4] 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. 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.

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

Annex B
(informative)

Cloud Computing Standards Initiatives

B.1 Standards for the Cloud

Standards provide a critical underpinning of the Cloud, across a broad range of topics such as data security and protection, interoperability, portability and e-Identity. While the Cloud standards landscape is still evolving, it is likely to emerge as a global framework comprising a mosaic of new standards, adaptations of existing standards combined with established standards, for example ISO/IEC 27000 series in the IT security area.

The National Standards Authority of Ireland (NSAI) retains prime responsibility for Ireland's standards system and is a key participant in the international standards system, being the National Body of ISO, the International Organization for Standardization, and the National Committee of IEC, the International Electrotechnical Commission. Currently, the main international cloud standardization work is happening under ISO/IEC Joint Technical Committee 1, Sub Committee 38 [JTC 1/SC 38 – Distributed application platforms and services (DAPS)]. SC 38 is driving international standards initiatives in Cloud, but also in web services and in Service Oriented Architecture (SOA – systems for designing and developing software in the form of interoperable services). NSAI, through its ICT Standards Consultative Committee (ICTSCC), maintains active engagement across all relevant Cloud domains covering Cloud Computing, SOA, IT Security and IT Governance via relevant Irish mirror committees of the international JTC 1 system.

Emerging Cloud standards will likely focus on Cloud definitions, vocabulary, Reference Architecture, and use cases. Additional standards work is also underway in Green IT /Sustainability domain via JTC 1/SC 39 - Sustainability for and by Information Technology. Since the data centre is the physical manifestation of the cloud, it represents an important opportunity to leverage cloud migration to improve energy efficiency standards of IT systems, and thereby reduce energy use and CO_2 and other greenhouse gas emissions below levels associated with non-Cloud IT systems.

B.2 Industry initiatives

Cloud computing touches many different aspects of Information and Communications Technology. Worldwide we see a number of national and international Cloud computing initiatives: from industry consortia to formal standardization organizations. Sometimes these initiatives are focusing on specific viewpoints of Cloud computing, while at other times they deal with Cloud computing architectures or use cases.

The **ISO/IEC JTC 1 /SC 38 - Study Group Report on Cloud Computing**[6] investigated several of these initiatives and Table 1 shows a summary of current Cloud Computing industry initiatives at the time of this report.

[6] http://isotc.iso.org/livelink/livelink/fetch/-8913189/8913214/8913373/Study_Group_on_Cloud_Computing_final_report.pdf?nodeid=12096352&vernum=-2

Table B.1 – Summary of current Cloud computing industry initiatives

Industry Initiatives	Area of interest
ITU-T Focus Group on Cloud Computing	International standard organization
ISO/IEC JTC 1/SC 7	International standard organization
ISO/IEC JTC 1/SC 27	International standard organization
European Network and Information Security Agency (ENISA)	EU agency
ETSI Technical Committee (TC) CLOUD	European standard organization
CESI (China Electronics Standardization Institute)	Chinese standard organization
CCF (Cloud Computing Forum in Korea)	Korean industry consortium
KCSA (Korea Cloud Service Association)	Korean industry consortium
Japan Cloud Consortium	Japanese industry consortium
Open Grid Forum (OGF)	Industry consortium
Distributed Management Task Force (DMTF)	Industry consortium
Cloud Security Alliance (CSA)	Industry consortium
OASIS	Industry consortium
Object Management Group (OMG)	Industry consortium
Storage Networking Industry Association (SNIA)	Industry consortium
Cloud Computing Use Case Discussion Group	Ad Hoc
The Open Group	Industry consortium
Institute of Electrical and Electronic Engineers Standards Association (IEEE-SA)	Standards Development Organization
ATIS Cloud Services Forum	Industry consortium
TeleManagement Forum	Industry consortium
Cloud Industry Forum (CIF)	Industry consortium
OSGi Alliance	Industry consortium
Open Data Center Alliance (ODCA)	Industry consortium

Bibliography

[1] ISO/IEC 27001, Information technology - Security techniques - Information security management systems -- Requirements

[2] PCI DSS – Payment Card Industry Data Security Standard

[3] Data Protection Act 1988, amended 2003 - Protection of Privacy of Individuals with regard to Personal Data

[4] Cloud Security Alliance (CSA) – Security Guidance for Critical Ares of Focus in Cloud Computing V2.1

[5] Cloud Security Alliance (CSA) – Consensus Assessments Initiative Questionnaire (CAIQ)

[6] National Institute of Standards and Technology (NIST) – Definition of Cloud Computing

[7] ISO/IEC JTC 1 SC38 SGCC N 430, Study Group Report on Cloud Computing

National Standards Authority of Ireland

NSAI is the state standardization body set up under the National Standards Authority of Ireland Act 1996 to publish Irish Standards.

Revisions

Irish Standards are updated by amendment or revisions from time to time. Users of Irish Standards should make sure that they possess the latest versions.

NSAI's **Tailored updating service** is designed to meet your precise needs and is therefore the most efficient and cost-effective way of keeping ahead. For more details on the tailored updating service see:

Standards.ie
Tel.: +353 1 857 6730/1

Buying standards

NSAI and International publications can be accessed:

- at standards.ie
- by tel: +353 1 857 6730/1 or
- email: info@standards.ie.

Feedback on Standards

NSAI welcomes any comments on standards whether proposing an amendment, correcting an error or identifying an ambiguity. Please use the "About NSAI" and then "Contact us" buttons on the **NSAI.ie** home page to explain your comment.

Participation in developing Standards

NSAI Standards, whether of National, European or International origin, are drawn up by panels of experts. Persons with expert knowledge in any field where standardization work is taking place and who are interested in contributing to the work of the panels are welcome to make themselves known to NSAI. Please note that conditions apply. Click on the "Get involved in Standards Development" button in **NSAI.ie**