TECHNICAL REPORT

ISO/IEC TR 22678

First edition
2019-01

Information technology — Cloud computing — Guidance for policy development

Reference number
ISO/IEC TR 22678:2019(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see http://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/JTC 1, *Information technology*, Subcommittee SC 38, *Cloud Computing and Distributed Platforms*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Cloud computing has become a major industry throughout the world in recent years, and today comprises a global network of large and small datacentres and telecommunications networks, operated by many different cloud service providers, offering vast numbers of different cloud services to their customers. These cloud services range from simple email and productivity applications, through replacements for traditional on-premises software, up to advanced services that cannot be constructed in any other way, such as social networks, big data processing, machine learning, and cognitive services.

Cloud computing offers many benefits to cloud service customers, to governments, and to society.

As with all commercial services, governments and enterprises are adopting policies to ensure that customer and governmental interests are protected.

This document provides information to assist with the development of such policies concerning the deployment and use of cloud computing systems and services.

Information technology — Cloud computing — Guidance for policy development

1 Scope

This document provides guidance on the use of international standards as a tool in the development of those policies that govern or regulate cloud service providers (CSPs) and cloud services, and those policies and practices that govern the use of cloud services in organisations.

This includes material that explains cloud computing concepts and the role of cloud computing international standards in formulating policies and practices.

The document makes references to various international standards. Where possible, these standards are ISO/IEC standards. Where a suitable ISO/IEC standard is not available, references are made to documents published by other WTO-registered standards bodies.

As explained in the WTO Agreement on Technical Barriers to Trade (TBT), standards play a vital role in supporting technical regulations and conformity assessment, however this document does not cover matters of trade.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 17788, *Information technology — Cloud computing — Overview and vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 17788 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
cloud computing
paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand

Note 1 to entry: Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

[SOURCE: ISO/IEC 17788:2014, 3.25]

3.2
jurisdiction
geographical or corporate area over which a cloud computing policy extends

Note 1 to entry: In a government policy context this will generally be the geographical area over which the body enacting the policy has legal authority either as government or as authorised regulator. However, in an enterprise or government agency environment, the jurisdiction of a policy might cover a business function, department, agency, or other organisational area of responsibility not tied to geography.

4 Abbreviated terms

CSC	Cloud Service Customer
CSN	Cloud Service Partner
CSP	Cloud Service Provider
CSU	Cloud Service User
DDoS	Distributed Denial of Service (attack)
DPA	Data Protection Authority
EN	European Norm
EU	European Union
IaaS	Infrastructure as a Service
ICT	Information and Communications Technology
IEC	International Electro-technical Commission
ISO	International Organisation for Standardisation
IT	Information Technology
ITU	International Telecommunication Union
ITU-T	ITU Telecom sector (responsible for standardisation)
JTC1	Joint Technical Committee 1 (a joint project between the ISO and IEC on standards for ICT)
MLAT	Mutual Legal Assistance Treaty
PaaS	Platform as a Service
PII	Personally Identifiable Information
SaaS	Software as a Service
SC 27	Sub-committee 27 of JTC1, responsible for information security standards
SC 38	Sub-committee 38 of JTC1, responsible for cloud computing standards
SLA	Service Level Agreement
SLO	Service Level Objective

SME Small or Medium sized Enterprise

SQO Service Qualitative Objective

WTO World Trade Organisation

5 Summary of this document

5.1 Purpose of this document

The purpose of this document is to ease the formulation of government and enterprise policies that facilitate the adoption and use of standards-based cloud computing services.

By following the guidance in this document, developers of policy can:

— leverage international standards in an appropriate fashion when developing policy;

— achieve greater global consistency in applicable laws, regulations and policies;

— reduce costs for CSPs and CSCs;

— increase choice and competition;

— simplify the challenges of deploying and adopting cost effective local, multi-national, or global cloud services.

5.2 Intended audience

— Lawmakers (in both developed and developing countries) at every level;

— Regulators, including Data Protection Authorities (DPAs);

— Those developing enterprise policies including:

  — Cloud service customers (large and small) and prospective customers,

  — Cloud service providers,

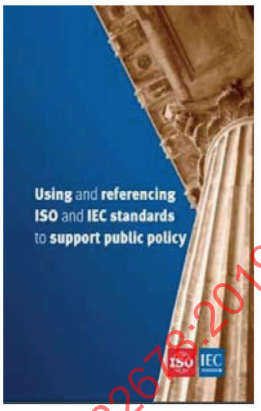
  — Cloud service partners;

— Those developing non-governmental rules and policies about trust and transparency for cloud computing, such as trade bodies and engineering institutions;

— Organisations that provide advice to governments and enterprises on the economic and political implications of technology policies, e.g. the Organisation for Economic Co-operation and Development (OECD).

In particular, this document is intended to assist those in smaller administrations such as local government, developing countries and those lacking in specialist knowledge on these topics.

5.3 How to use this document



This document provides guidance on which specific international standards might be applicable for policies on cloud computing and provides guidance on how they can best be employed. As such this document should be used in accordance with the overall ISO/IEC advice in this area as follows:

"The International Standards developed by the IEC and ISO are voluntary. And while they do not seek to establish, drive or motivate public policy, regulations, or social or political agendas, they can certainly provide valuable support to the implementation of public policy."

This statement comes from the publication "**ISO/IEC: Using and referencing ISO and IEC standards to support public policy"**, which is publicly available and can be found at: https://www.iso.org/iso/PUB100358.pdf

Please refer to this ISO/IEC publication for general advice on how international standards can be incorporated in the public policy process and, by extension, in the development of cloud computing procurement policies for both public and private organisations.

6 Understanding cloud computing aspects for policy development

6.1 Introduction

This clause provides an explanation of some key characteristics and implications of cloud computing where an understanding is desirable by those developing public or corporate policy for cloud services. The intent is to present this material in a readable and approachable manner for those who are not full-time cloud computing engineers, while providing references to more technical material which can be considered when appropriate.

6.2 Cloud computing essential characteristics

6.2.1 Standard definition of cloud computing

The definition for cloud computing (3.1) captures several essential characteristics that differ from traditional, local, or hosted computing. These characteristics are further explained in ISO/IEC 17788 and will be described in even greater detail in the forthcoming ISO/IEC 22123[1)].

Effectively, this definition says that cloud computing involves the provision of almost any ICT resource as a service (a *cloud service*) over the network, and that this provision can be done dynamically on-demand at the CSC's request, much like the way utilities, such as telecommunications, are provided. Customers use what they need when they need it, and consumption is billed accordingly. ICT resources can be accessed almost as simply as pressing a switch to turn on a light, and can be released almost as simply as pressing the switch again to turn the light off. The need for the CSC to perform the lengthy processes to acquire, install, configure, secure and operate hardware, software and applications is greatly reduced, if not entirely eliminated.

6.2.2 Essential characteristics of cloud computing (from ISO/IEC 17788)

Cloud computing has a series of essential characteristics, which are summarized in Table 1.

1) Under development. Current stage: 30.60.

Table 1 — Cloud computing essential characteristics

Characteristic	As seen in cloud computing
Broad network access	The cloud service can be accessed from an arbitrary location by a wide variety of device types including PCs and mobile devices of all kinds, connected in many ways, usually by the Internet but sometimes by private networks, such as a corporate internal network.
Measured service	Customers' use of the cloud service is measured, and they might be charged based on what they really use, much as electricity supply is often billed based on measured energy consumption. Reduced usage can therefore mean reduced cost.
Multi-tenancy	Multi-tenancy means the resources supplied by a cloud service are shared by multiple CSCs. Each tenant's use of the resources is isolated and inaccessible from all other tenants — so that CSCs are assured that their data and their use of applications cannot be seen by any other CSCs. This is comparable to the expectation that details in a bank account are not visible to other customers of the bank. Note that a single customer can sometimes have multiple, different tenancies with a given cloud service, e.g. where the activities of different departments in an organisation need to be kept isolated from each other. Note also that while a private cloud by definition has only a single CSC, that single customer might still choose to employ multiple tenants of their own for isolation purposes.
On-demand self-service	Generally, cloud services allow the customer to sign up, pay for, and make use of the service without needing to interact with a human customer service representative. Customers are generally also able to manage their service, or cancel it, again without requiring human intervention. There might be exceptional circumstances where interaction with a human operator is required, but these will be abnormal cases, not regular business practice.
Rapid elasticity and scalability	Cloud services are able to allocate resources dynamically to a particular workload as needed. This is sometimes described as scaling up (increasing the size of a single resource), or scaling out (allocating additional similar resources). The intent is that customers can expand and contract their use of the cloud service as dynamically as possible, often to cope with planned or unexpected increases or decreases in workload. For example, if a website hosted on a cloud service suddenly attracts a huge amount of interest, the website owner can order (and pay for) more computing power and bandwidth so their site isn't overloaded. Once the peak is past, the resources can be released and the cost reduced. Another important aspect of cloud service scalability is that the resources available can appear effectively unlimited to the customer. This is in contrast with traditional datacentres, where the number of servers, the amount of data storage capacity, the network bandwidth all typically have limits that can only be changed by installing more equipment.
Resource pooling	Cloud computing gains efficiency by sharing various resources between multiple tenants and workloads. As an example, in traditional computing, ten customers might be hosted on ten separate servers, even if each of them was only using half of each server's capacity. In a cloud computing environment, those ten customers could be automatically provisioned onto just five servers

To explore the inter-relationship between these six essential characteristics and the various implications of cloud computing identified in this document, see Annex A.

6.3 Major benefits of cloud computing

6.3.1 Benefits for cloud service customers (CSCs)

The benefits enjoyed by CSCs are summarized in Table 2.

Table 2 — Customer benefits of cloud computing

Benefit to customer	As seen in cloud computing
Low capital investment	A customer wishing to develop or run a new application no longer needs to provision their own IT equipment, nor the buildings and infrastructure needed to house and support it, and potentially does not need to acquire, install and operate much or all of the software stack for the application. The customer is able to pay a relatively small amount (i.e. no need to buy server equipment) while developing and/or deploying the new application, then gradually build up the amount of cloud server resources they use as the usage of the application and revenue stream increases.
Cost-effectiveness of cloud scale	CSPs are able to purchase at scale, meaning that servers and other resources are much cheaper when bought in huge quantities. These cost savings can be passed on to the individual customers. Also, the cost per server of running very large datacentres, in terms of manpower, energy and other costs, is much lower than in hundreds of small installations.
Use as needed	Cloud services allow customers to start small, then ramp up and down very quickly as needed. The customer can reduce their bills during "quiet" periods for their business, and increase capacity in readiness (or in response to) peak loads such as for seasonal shopping or unexpected popularity.
Competition	Cloud service prices are very competitive due to the dynamics of the market. Each new project has a choice of which CSP to use, and new start-ups continue to challenge the big operators with special features and innovations.
Security	At one time, security was seen as a concern with moving to use cloud services, but today it is seen as a significant strength. Security is no longer considered as a significant hurdle in adoption of cloud computing. There are several reasons for this. Firstly, reputable CSPs often have security teams working around the clock and around the world to keep their systems secure, up to date with security patches, and ahead of any emerging threats that can be identified. They are very quick to respond to incidents. Even large commercial enterprises and smaller governments will struggle to recruit and pay for an equivalent level of 24×7 security expertise on their own staffs. Secondly, one of the biggest threats to computer security is the "insider" attack, where someone with administrative or physical access is involved in the breach, perhaps a corrupt or disgruntled employee, but who would not have the same kind of access to an external cloud service. (See ITU-T X.1601).
Availability and Reliability	Many CSPs operate multiple datacentres in separate locations and this offers customers the opportunity for improved availability of their applications and data. Applications can be run in multiple datacentres, and data can be replicated between those datacentres, avoiding any single point of failure. If one datacentre is taken offline by some natural disaster or major failure, CSC access to applications and data can be switched instantly to another datacentre.
Advanced capabilities	It is increasingly the case that CSPs are making advanced capabilities available as off-the-shelf cloud services. Examples include AI systems, advanced Analytics, and Big Data services. Some of these services are pre-trained on vast datasets. CSCs might struggle to implement these advanced capabilities in-house, due to limited access to the skilled people and resources. It is often far more cost-effective to integrate these advanced cloud services into new applications built by the CSC.
Choice of cloud service deployment models	Cloud computing allows a CSC to choose the most appropriate deployment model to meet their requirements, including public, private, community and hybrid cloud service deployment models (see ISO/IEC 17788). For a private cloud deployment model, the CSP will be part of the CSC's own organisation.
Easier compliance	Most public cloud CSPs obtain a variety of certifications for their cloud services. By taking advantage of these cloud services, a large part of the burden of obtaining certifications and ensuring compliance can be lifted from the CSCs. Also, CSPs often provide advice, guidance and support for their CSCs who are seeking to have their use of the cloud service comply with such things as privacy and data protection regulations in their jurisdiction.

6.3.2 Benefits for society

The benefits for the wider society that can flow from cloud computing are summarized in Table 3.

Table 3 — Benefits to society from cloud computing

Benefit to society	As seen in cloud computing
Energy efficiency	Large purpose-built datacentres can be far more energy efficient than many smaller ones. They can also be in places where power is more readily available at a lower cost, or where the power used is based on renewable energy. Some datacentres are even designed to operate on free-air cooling, which greatly reduces the energy requirement. In addition, CSPs are able to optimise their customer's workloads and data on to the minimum needed number of servers[a].
Robustness and Resilience	Connections to cloud services are robustly protected, and far less vulnerable to virus or other malware attacks. They are also often strong enough to withstand determined distributed denial of service (DDoS) attacks from hackers and botnets. Cloud service providers often offer geographic diversity, such that cloud services can continue even in the event of a major natural disaster disabling one of their datacentres. Further, because these systems generally use software to provide resilience across multiple physical machines, they do not require every computer to run reliably. For a large cloud service datacentre, there is no need to carefully tend every server. Rather, workloads can be moved without impact to the customer. The service remains resilient even if the individual servers are not. The failed equipment can then be reconditioned and reused or recycled as appropriate. The resilience of cloud services benefits society, because CSCs no longer depend on their own resources and skills to keep business processes running.
Lawful access	While customer privacy is important, society also needs to protect itself from bad actors. When data is stored in cloud services, rather than on local computers, there are additional measures to obtain properly authorised legal access to it for criminal investigations, anti-terrorism, and other government purposes. However, this is not a panacea, and both legal and engineering challenges remain. For example, a situation where data is stored in (and/or managed from) another jurisdiction might involve legal complications for investigators, such as requiring the use of a Mutual Legal Assistance Treaty (MLAT) to obtain the cooperation of appropriate authorities in the other jurisdiction. A related area is e-discovery during legal proceedings, for which international standards such as the ISO/IEC 27050 series of standards could be helpful.

[a] A small business moving to the cloud could reduce its energy consumption and carbon emissions by more than 90 %, by running its business applications in the cloud instead of running those same applications on its own infrastructure.

Source: Bibliography [39]

6.4 Implications for policy makers

6.4.1 Shared responsibilities

Due to the nature of cloud computing, where the CSC and the CSU have considerable control over the use of the cloud service, there are *shared responsibilities* to maintain the security, privacy, confidentiality, and integrity of the service. For example, CSCs remain responsible for following best practices in their use of the cloud service, such as in handling passwords or other credentials, in giving appropriate permissions to specific users, in the type of data they put into the cloud service, and in labelling content so that it can be treated correctly by the cloud service. Such practices determine the overall security, privacy, confidentiality and integrity of the service, but are beyond the control of the CSP alone.

The use of industry-defined codes of practice to guide both the CSP *and* the CSC in the operation and use of cloud services is widely held to be a valuable approach.

6.4.2 Cloud services which are deployed and managed across multiple jurisdictions

Traditionally, IT systems were deployed within an organisation, or within a hosted environment dedicated to a single country or other jurisdiction. Even international telecommunications infrastructures were constructed country by country, with clear interconnection points defined at international boundaries, such that resources and management were normally done by staff and using facilities in the same jurisdiction as the customers of the service. This is no longer true for many cloud computing systems and services.

Global and multinational cloud services achieve scale and efficiency by centralising their activities, management and staff as much as possible. This means that customers in one country might be using cloud service resources (e.g. servers, data stores and network equipment) that are located in another country, with those servers being managed from a third country.

This approach provides many benefits to both CSP and their CSCs.

1) Having a single global version of the software suite for the cloud service means that a single development, testing, and security team can support the CSP's entire network of datacentres, no matter how many there are or how many countries they are located in.

2) CSPs and CSCs benefit from continuous, timely improvements to the service, rather than each country or datacentre having to implement updates individually.

3) Security patches and fixes can be deployed more easily. Vulnerabilities or breaches identified anywhere can be addressed everywhere simultaneously.

4) It allows for geographic diversity in the deployment of services and data. This can provide redundancy and protection against major incidents such as flooding, earthquake or network failure, which can take an entire datacentre out of service. It is rarely cost effective or efficient to provide multiple datacentres in smaller countries, so out-of-country redundancy might be the only option for meeting business continuity requirements.

5) For data that is not geographically constrained, the cloud service can dynamically move or copy data between datacentres to optimise performance and storage utilisation. For example, some data might be relevant for reading worldwide, perhaps on mobile devices (e.g. maps, news, video), such that global replication greatly improves the customer experience by reducing data access latency. Such data movement and replication is usually fully automated based on objective measurements of data usage behaviours.

6.4.3 Economics of managing a global cloud service

CSPs, especially large organisations, are resilient and flexible to minimising the cost of their capital investments and operational costs, and possibly enabling lower pricing of their cloud service offerings. CSPs ordinarily use standard equipment configurations across their datacentres allowing them to purchase equipment in large quantities. Servers used in cloud datacentres ordinarily are devoid of many of the "bells and whistles" found in off-the-shelf servers which saves costs and energy. CSPs mostly use software-based resiliency rather than equipment redundancy to provide business continuity further reducing capital and operating costs. For a large cloud service datacentre, the problem is therefore not "keep all the equipment running", but rather to relocate workloads such that the CSC does not notice any hardware failures or changes to the service. Such resiliency may require applications to utilize particular software architecture styles or design patterns relating to e.g. "cloud native" applications in order to make failures transparent to cloud service users.

Because of the scale of large cloud datacentres, CSPs design for minimum energy use to save costs and maximize computing density in a way that smaller datacentres cannot. Cloud servers have no need for interfaces (such as for monitor, mouse and keyboard) which are never used in a bulk rack-mounted server design. Additionally, CSPs are incentivised to design highly efficient cooling and power distribution systems that lower environmental impact. CSPs initiate bespoke renewable energy projects to power their datacentres and they can employ advanced, environmentally friendly power sources such as bio-mass fed fuel cells. Besides renewable energy, depending on the location, heat recycling can

be used to collect and utilize generated heat to, e.g. warm local housing. These and other techniques are available and measurable in all energy-efficient datacentres as covered in standards such as ISO/IEC 19395 and ISO/IEC 30134-4, developed in ISO/IEC JTC 1, Subcommittee 39, *Sustainability for and by Information Technology*.

Using a single version of software across datacentres is another way CSPs contain costs. Therefore, a CSP will endeavour to use the exact same software for each service throughout their network of datacentres. This software can then be monitored, managed and maintained by a single team (including security analysts). New versions of software will be tested and rolled out gradually, to reduce the risk of introducing a catastrophic error to the whole network, but the goal will remain to keep a single deployed software version throughout the CSP as much as possible.

Where multiple software versions exist, any changes will need to be tested against all active versions, and any security vulnerabilities have to be checked and patched in every version. Also, extensive testing is required when software of one version interacts with software of another version. As such, the cost of maintenance rises approximately with the square of the number of versions in use.

Consistency of hardware and software further enables the automated management of cloud services. CSPs can use multiple ways (e.g. artificial intelligence) to monitor millions of servers and processes to detect impending failures and anomalies. This increases business continuity and reduces costs for CSPs and CSCs.

6.4.4 What global, scalable public cloud computing makes possible

Globally deployed, highly scalable public cloud services offer cost effective and scalable services across geo-political boundaries. Such services offer possibilities that were not available in traditional on-premises deployments or private clouds. For example, such global services enable collection and transfer of user data as well as organisational data across geo-political boundaries. The volume and speed of data collection and transfer are unprecedented.

With the introduction of data analytics and machine learning techniques using the power of public cloud services and large quantities of collected data, more than ever before the provenance and categories of data need to be understood. In addition, as data gets aggregated and de-identified (see ISO/IEC 19944), public and enterprise policy developers need to understand the necessary concepts, terminology and tools to communicate the desired behaviours and outcomes to protect individuals as well as protect confidential organisational data.

6.4.5 Implications of service scale and velocity

A key characteristic of cloud computing is that the service is "On-demand self-service" (see ISO/IEC 17788:2014, 6.2). This means that customers can create an account, pay for the selected service(s), start using it, post content, make changes, or whatever else the cloud service provides for them, in a highly automated process. This speed of using the service is highly valued by CSCs, and has been a major driving force in cloud service adoption. However, it is also challenging for CSPs to filter out "bad actor" behaviour by CSCs. Examples of such bad behaviour include using the cloud service for malicious purposes (e.g. spreading malware, sharing illegal or extreme content, copyright violation, etc.), careless use (e.g. putting confidential information in unsecure places), or ignorant use (e.g. posting content which is acceptable in their home country, but inappropriate or illegal elsewhere).

While CSPs constantly work to mitigate these bad actors, it remains an "arms race" between the CSPs and malicious (authorised or not) CSUs. CSPs have been deploying both human specialists and artificial intelligence tools to mitigate improper use of their services.

CSCs, where applicable, assume responsibility and management of the access control and the use of their environment. As an example, the CSC needs to control authorization and authentication to their cloud services to ensure that their CSUs do not abuse cloud services. Further, the CSC needs to monitor content and usage of their cloud services to ensure that all applicable local, national and international laws are respected (see also 6.4.1).

6.4.6 Implications of continuous development

In pre-cloud computing, software was developed in terms of large "releases", often two or more years apart. This approach allowed large amounts of testing and certification to be performed before each release went live. In practice, updating from one release to the next often required systems to be taken down, updated with new code, and put back up again, either at once or in batches of machines thus causing planned interruption of service. Should an update fail, the whole process might need to be reversed. This also meant that security updates might have to wait weeks or months for a "service pack" or other software update opportunity to be deployed.

Cloud computing, due to its 24×7 operating nature and the modern security threat environment, has moved to a model of continuous development where small incremental changes are introduced very frequently, often weekly or even daily. Security fixes can be rolled out even more rapidly when needed.

The effect of this is that there is no longer a clear "release" schedule with long periods available for rigorous planned testing or certification processes. A traditional approval cycle for a legacy system would not be completed on a cloud system before it was already migrated to a new version, and with further changes already on the way. Therefore, testing and certification needs to adapt to an environment of constant software changes. ISO/IEC 27001 provides structure for such testing and certification of rapidly innovative technology. One effect is that testing can be more focused. It is certainly possible that a few errors get through the service provider's own checks to impact customers. However, it is equally true that a fix for such a problem can be deployed much more quickly.

6.4.7 Implications of multi-tenant cloud services

Because cloud resources such as computers, storage, and networks are pooled resources shared by many CSCs and/or tenants (see 6.2.2), it is no longer possible to give commercial auditors or government inspectors physical access to equipment specific to one CSC without potentially violating the confidentiality of other CSCs using the same pooled resource. Some data might be spread across multiple shared storage resources using "sharding".

In any case, the CSC controls their own data, and the CSP might not be able to view or control specific data in a customer's cloud datastore, for example if it is encrypted.

This also means that fully secure data deletion, which under some older policies can require the destruction of the storage media, cannot be performed as frequently or rapidly as in single-customer systems. Where the data of one customer occupies only 10 % of the space on a disk drive, it is neither economic nor efficient to lose the use of it for other customers until the drive is eventually taken out of service.

See ISO/IEC 19944:2017, 9.2.8.2[2)] for a description of a layered approach to secure deletion that does not require destruction of media.

When it comes to issues of lawful enquiry, again physical access to resources shared by a large pool of users is not the appropriate approach. Rather, a cloud-oriented approach that relies on the capabilities of the cloud services to support inquiry and destruction is required. In many instances, application-level cloud-based log data can provide session access and activity details to support auditing, logging, and forensics.

6.4.8 Implications of geographical restrictions

CSPs with larger and global operations, will have various approaches for storage of static data. When a customer chooses to store (or generate) data, the CSP needs to make smart decisions over where it will be physically stored. Considerations that go into this decision include:

— Customer or legal requirements or policies.

2) A useful reference from ISO/IEC 19944 is Joel Reardon, David Basin, Srdjan Capkun, SOK: Secure Data Deletion, *IEEE Symposium on Security and Privacy*, 2013, available from <http://www.ieee-security.org/TC/SP2013/papers/4977a301.pdf>.

— Currently available storage capacity (e.g. for very large amounts).

— Storage performance (the nearest datacentre might be very busy due to other customers, resulting in slower data access and bandwidth than might be possible from a less loaded but more distant datacentre).

— Storage costs (storage in some places can cost the CSP more than in others, for example due to differences in energy costs, or other operating costs).

— Network capacity and availability (sometimes there is better connectivity to a distant location than to a local one)[3].

— CSCs can be subject to business continuity (disaster recovery) policies and regulations which require them to maintain geo-redundant copies of their data. In smaller jurisdictions it might not be possible to provide geo-redundant storage within the jurisdiction. It is also ordinarily required that geo-redundant resources be placed at a distance adequate to prevent failure of both the primary resource and the geo-redundant resource from large scale natural and man-made disasters.

— Many CSCs have field staff, customers, suppliers, and/or partners located in other parts of the world. For these users, having the data they need stored more locally to them can improve the performance of the service.

— CSCs might choose to collect and process data at a local level and consolidate their data from locales in a larger scale facility in a different jurisdiction. This is sometimes done to reduce network latency concerns, and sometimes to reduce the volume of data that needs to be transferred to the central datacentre (e.g. from thousands of mobile apps, IoT devices, or other data collection sources).

— Geographic restriction of data does not always prevent data leaving the restricted location since most security vulnerabilities are exploited remotely. Internal resources and manual misconfiguration of data can also account for loss of data; the last two can be mitigated in a more efficient global cloud environment.

Some policies, both governmental and enterprise, might require that some or all data stored in a cloud service is physically kept within a specific jurisdiction.

For the reasons given above, data that is geographically constrained in this way might be somewhat more expensive to store due to management overhead, less storage efficiency, and might also suffer reduced application performance due to network latency or bandwidth bottlenecks.

For smaller jurisdictions there might be very few CSPs with a local datacentre. Even if there is one, there might be no possibility of offering geographic redundancy with only a single datacentre in the relevant jurisdiction. This might increase vulnerability to any local catastrophe. See 6.3.10.

6.4.9 The need for cloud service data categorisation and classification

Cloud services hold large amounts of data, both belonging to the CSP and that of their customers. It is useful to categorize data to improve its use and management. ISO/IEC 17788 provides three basic categories of cloud data, while ISO/IEC 19944 expands those categories to four top-level categories and also provides a detailed taxonomy for many different sub-categories.

The four top-level categories are as follows:

— Cloud Service Customer Data (which is provided or generated by the CSC themselves, such as documents, databases, designs, client lists, staff personnel records, etc.)

— Cloud Service Provider Data (which concerns the operations of the cloud service, and is irrelevant to CSCs, such as equipment configurations, network routes, maintenance records, CSP staff rosters, etc.)

3) As an extreme example, one major video game company launched a latency-sensitive service on the USA's east coast from a datacentre located in London, England rather than their existing one on the USA's west coast. This was because connectivity across the Atlantic Ocean performed much better for latency than across the mainland USA.

— Cloud Service Derived Data (which arises from the customer's use of the cloud service, such as records of their activity, call logs, audit logs, etc.)

— Account Data (such as CSC contact and payment information)

On any given cloud service, all of these categories will be present and all can potentially include some PII for the purposes of Data Protection and Privacy law.

A policy approach that applies appropriate rules to specific, limited, and clearly defined categories of data (such as those enumerated in ISO/IEC 19944) allows for much more efficient data management, and thus cost-effectiveness of the cloud service. It also makes the task of auditing for compliance much clearer.

For the Data Controller, concentrating appropriate restrictions on data which *does* contain PII is far more cost-effective and efficient than applying broad control to data categories which *could potentially* contain PII, since as noted above the latter group is *very* much larger.

(A Data Processor, by contrast, usually has no idea whether any given data contains any PII or not.)

As another example, for non-PII data there is a very big difference in suitable handling of current, confidential, or valuable information and that of outdated, public, or valueless data.

See also 6.4.1 with respect to CSC and CSU responsibility for achieving assurance in the security of cloud services to safeguard public sector and regulated workloads.

6.4.10 Interoperability and portability

Firstly, it is important to understand that these two terms have very different and distinct meanings. In simple terms:

Interoperability is the ability of two connected systems to exchange information, and to mutually use the information that has been exchanged. For example, a PC and a printer are interoperable if the PC can send a document to the printer for printing and the printer can understand the format and content of the document.

Portability comes in two forms:

— Data portability is where *data objects* (such as documents, images, files, or databases) can be copied or moved from one system to another, and can still be used on the second system.

— Application portability is where *executable software* can be copied or moved from one system to another, and can still be used (run) on the second system.

Interoperability and portability are highly complex multi-faceted topics, and the details are addressed extensively in ISO/IEC 19941.

6.4.10.1 Considerations for interoperability in a cloud computing environment

ISO/IEC 17788:2014, 3.1.5 defines interoperability as the ability of two or more systems or applications to exchange information and mutually use the information that has been exchanged. In the context of cloud computing, interoperability is further described as a cross-cutting aspect providing the ability for a cloud service customer system to interact with a cloud service and exchange information according to a prescribed method and obtain predictable results (see ISO/IEC 17788:2014, 6.6). Interoperability also includes the ability for one cloud service to interact with other cloud services (see ISO/IEC 17789:2014, 8.5.5 and ISO/IEC 19941).

Interoperability and portability in cloud computing is rarely confined to a binary decision of possible or impossible. Interoperability is potentially subject to implementation costs. A cost/benefit analysis is required to determine whether the resources needed to assure exchange of information in the prescribed method while obtaining predictable results is worthwhile. The ability of systems of a CSC and cloud services as well as multiple cloud services to interoperate is more than a matter of investing

the resources to assure the exchange of information between the interfaces at either end. In addition, any changes caused by interoperation requirements might entail additional training for end users, management and operations staff.

There are many considerations when addressing cloud interoperability. These include:

— the ability of a CSC to interact with a cloud service by exchanging information according to a prescribed method obtaining predictable results;

— the ability for a cloud service to work with other cloud services;

— properties needed to facilitate successful interactions between an organisation's ICT facilities and a cloud service;

— roles and activities as defined in ISO/IEC 17789;

— cloud capabilities types as defined in ISO/IEC 17788;

— interfaces between different functional components as defined in ISO/IEC 17789:2014, 9.2.

6.4.10.2 Considerations for portability in a cloud computing environment

In the context of cloud computing, portability refers to the ability of a CSC to move and suitably adapt their applications and data between the CSC's systems and cloud services, between different cloud deployment models, and between cloud services of different CSPs. ISO/IEC 19941 provides considerations for cloud application portability and cloud data portability separately.

Portability is "possibly subject to switching costs". A cost/benefit analysis is required to determine whether porting applications and/or data is worthwhile. The similarity of the CSC and CSP's systems is therefore more a matter of lowering the switching cost than of "enabling" portability to take place, since almost any portability is possible if the customer is willing and able to pay for it. Switching concerns are not limited to costs; it also usually involves some risks and usually entails the CSC spending effort and time and perhaps a period of service interruption.

There are many considerations when addressing portability in cloud computing. These include:

— allowing CSCs to migrate applications and data in response to business needs such as faster service, lower cost, greater reliability or disaster recovery needs;

— wider availability of application and data allowing access to a broader market;

— time and effort required for porting both applications and data, however, such overhead can be reduced using common programming languages, standards, tools, frameworks, models, run times and APIs;

— limiting of lock-in situations where the CSC is tied to the cloud services of one CSP.

In general, CSPs endeavour to provide some degree of interoperability and portability between their products and those of their competitors. This is in their own commercial interests as a means to convince potential customers. However, the engineering challenges must not be underestimated.

6.4.11 Trust and transparency

CSPs have recognised that customer and regulatory trust in their cloud services is essential for commercial success. One definition of a "trusted cloud service" (there are others) is as follows:

trusted cloud service: A cloud service that satisfies a set of requirements such as transparency for governance, management and security so that a cloud service customer (CSC) can be confident in using the cloud service. (Source: ITU-T Y.3501, 2016).

NOTE 1 The set of requirements will vary depending on the involved cloud service customer, the nature of the cloud service and the governing jurisdiction.

NOTE 2 The set of requirements could also be related to additional cross-cutting aspects such as performance, resiliency, reversibility, SLAs, etc.

NOTE 3 Transparency means that the cloud service provider (CSP) should commit to the CSC that they have appropriate and clear control and reporting mechanisms for governance, management and security, such as SLA commitments, online announcements, data handling policies, etc.

This definition clearly shows that trust involves multiple aspects.

Transparency — To be trusted, a CSP needs to do the right things, but they should also be *seen* to do the right things. This includes things like compliance with relevant standards, regulations and policies, often verified by certification and audit (see 6.4.13). It can also include providing statements and reports in industry-standard formats using standardised terms (e.g. ISO/IEC 17788, ISO/IEC 19086 series, ISO/IEC 19944, ISO/IEC 27017, ISO/IEC 27018) so that customers and regulators have a clear basis for comparison and understanding.

Security — CSPs should implement an appropriate level of security for the service being offered. For a free-to-play cloud-based online game, this might not be much, but for any service handling personally identifiable information, especially sensitive information such as financial or medical information, the security requirements will be very much higher.

Management — The cloud service's management system should be capable of handling the CSCs requirements and the CSP's various compliance obligations. For example, a cloud service which is very secure but which is unable to correctly constrain customer data to reside in the correct jurisdiction(s) cannot be trusted.

Governance — A cloud service that has excellent security and effective management is still only as trustworthy as the governance of the organisation. For example, a CSP where the CEO is able to make changes to their data handling policies on a whim to meet a new business opportunity (e.g. by selling the data), cannot really be called trustworthy. Transparency of governance might be addressed by certification of compliance with international standards in this area such as ISO/IEC 38500.

As stated in the Notes above, these aspects are highly contextual and it would be difficult if not impossible to create a one-size-fits-all set of criteria or regulations for all.

6.4.12 Exceptional circumstances

Some CSPs have greater capacity and resources in sustaining and surviving large scale disasters such as earthquakes or floods that could damage one or more datacentres, or isolate them from the network. However, when there is only a single such facility within a jurisdiction it might be appropriate to consider the possible impact should it suffer a serious outage whether by natural or human causes.

If a policy requires a cloud service to restrict some data or applications to the local jurisdiction (see 6.4.8), it might be appropriate to consider an allowance for exceptional circumstances.

The policy setting organisation needs to evaluate in each case whether it is better to maintain the geographic restriction, thereby risking business continuity, or whether it is allowable for the CSP to continue offering the service from a datacentre in another jurisdiction until normal service can be resumed. This is not a decision that can be made *after* a disaster hits, since the CSP will need to have made prior arrangements for the handover before the original datacentre is lost or isolated. For example, a CSP might offer a mechanism for keeping encrypted backups of data in another part of the world, such that they can be decrypted and brought into service only under such exceptional circumstances.

The cloud SLA is intended to be useful for CSC and CSP to make clear the criteria of exceptional circumstances.

6.4.13 Compliance, certification, audit

Some (though not all) of the standards for cloud computing are designed to be used for independent certification of a CSP, or indeed a CSC[4]. These standards provide clear criteria for an auditor to measure against.

There is value in leveraging internationally-recognized accreditations to avoid re-doing audit work under new certification regimes. Re-using work already performed by an accredited assessor promotes a globally harmonized approach.

Examples include ISO/IEC 27001 together with ISO/IEC 27017 and ISO/IEC 27018 which covers risk-based security of personal information stored in the cloud.

A CSP who seeks and obtains certification against these standards can demonstrate that they have been assessed and audited by independent professionals and can be trusted to follow the (internationally) standardised best practice correctly.

Once a certificate of compliance to a suitable standard is granted, ongoing compliance to the requirements is assured by internal processes and periodic external audits.

6.4.14 Challenges for small and medium sized enterprise (SME) adoption

Adoption of cloud computing services by small and medium sized enterprises (SMEs) has both advantages and challenges.

In general, SMEs using cloud services fall into two categories:

— Non-IT small and medium sized enterprises;

— IT-oriented small and medium sized enterprises.

6.4.14.1 Non-IT small and medium sized enterprises

Firstly, there are SMEs where IT services are incidental to their actual business, e.g. retailers, small manufacturers, farms, partnerships, professionals. This type of SME is most likely to choose cloud based applications that are tailored (or can be customised) to their own business needs, such as general office productivity applications (work processors, spreadsheets, document storage, accounting, stock tracking, telephony). In addition, they might use specialised applications designed for their particular industry, perhaps built by a cloud service partner (CSN — see ISO/IEC 17788).

For these SMEs, cloud computing greatly reduces the need to own, manage, and secure software other than that which resides on their own desktop PCs or other devices. They never need to see or worry about running or securing a server.

A key challenge is often obtaining cost-effective and reliable network connectivity (including sufficient bandwidth) to the CSP. This can be especially difficult in rural areas (even in otherwise highly developed countries) as there might be only a single network service provider with little incentive to invest, or perhaps none at all. SMEs in developing countries can be especially challenged in this regard. Published maps showing widespread broadband availability are sometimes misleading as they might include cellular coverage such as 3G and 4G which is often unsuitable or too expensive for continuous daily use of cloud services for SMB business. For SME staff out on the road, the use of WiFi hotspots can be useful, but even these can be frustrating if not well designed and maintained.

There are also challenges for SMEs trying to remain compliant with data protection and privacy rules who cannot afford expensive consultants or specialist employees to take care of this. Instead they must mostly rely on the advice and features provided by their CSP, which might or might not be easy to understand when it comes to meeting local law and regulations. However, cloud services could provide

4) Note that *not* all international standards are suitable for certification. For example, some describe terminology or standard concepts but do not include any requirements that can be verified by an auditor.

a better option than equivalent on-premises software, since it is more likely that the CSP would have access to the right skills to ensure compliance than an SME organization.

6.4.14.2 IT-oriented small and medium sized enterprises

Secondly, there are SMEs such as IT-oriented start-ups which opt for cloud computing as the platform for developing their new business. They can take advantage of getting started on minimal capital investment and then grow as gently or rapidly as their market opportunity allows.

A successful SME of this kind can rapidly gain cloud-based customers around the world, and provide a strong source of export revenue for their home jurisdiction. Some of these SMEs can grow into powerhouses of innovation and revenue, and even become influential throughout the whole business world.

While they are more likely to be based in cities and thus have better access to broadband than the first group, they can struggle with interpreting and anticipating how their new business model(s) might be understood and treated by regulators, especially if their approach is seen as disruptive to existing businesses or social norms.

6.4.14.3 Impact of large business policies on small and medium enterprises

Both kinds of SMEs can be disproportionately affected by policies that are crafted primarily around regulating large enterprises.

For example, a new regulation that might require the assistance of a lawyer and a specialist data-science contractor for a 10,000-employee large enterprise might *still* require a lawyer and a contractor for a 5-employee start-up business, which could be beyond the finances of the SME, or make their adoption of cloud computing impossible.

Any disproportionate impact on SMEs can have serious economic consequences in any places where SMEs make up a substantial part of the local business community. While large CSPs are far less directly affected, such a loss of local SME business can also adversely affect the large CSPs who provide the cloud service(s) for them, thus reducing the value of the entire local cloud ecosystem and depriving local people of some of the benefits identified above.

7 Using international standards to assist in developing policies that cover cloud computing

7.1 International standards relevant to cloud computing policy development

International standards created by ISO/IEC JTC 1 often build on each other, or at minimum reference material included in other standards. It is important to understand the inter-relationship of such standards, especially when it comes to those related to cloud computing. This way users of such international standards have an understanding for how they can use them in a set of comprehensive tools. For example, Figure 1 below shows how the foundational security and privacy risk management frameworks developed in ISO/IEC JTC 1 SC 27 are the basis for derived standards such as ISO/IEC 27018, or how ISO/IEC JTC 1 SC 38 standards ISO/IEC 19944 and ISO/IEC 19941 are derived from foundation cloud computing standards ISO/IEC 17788 and ISO/IEC 17789, and in turn they are referenced by various parts of the ISO/IEC 19086 series, describing cloud service agreements.

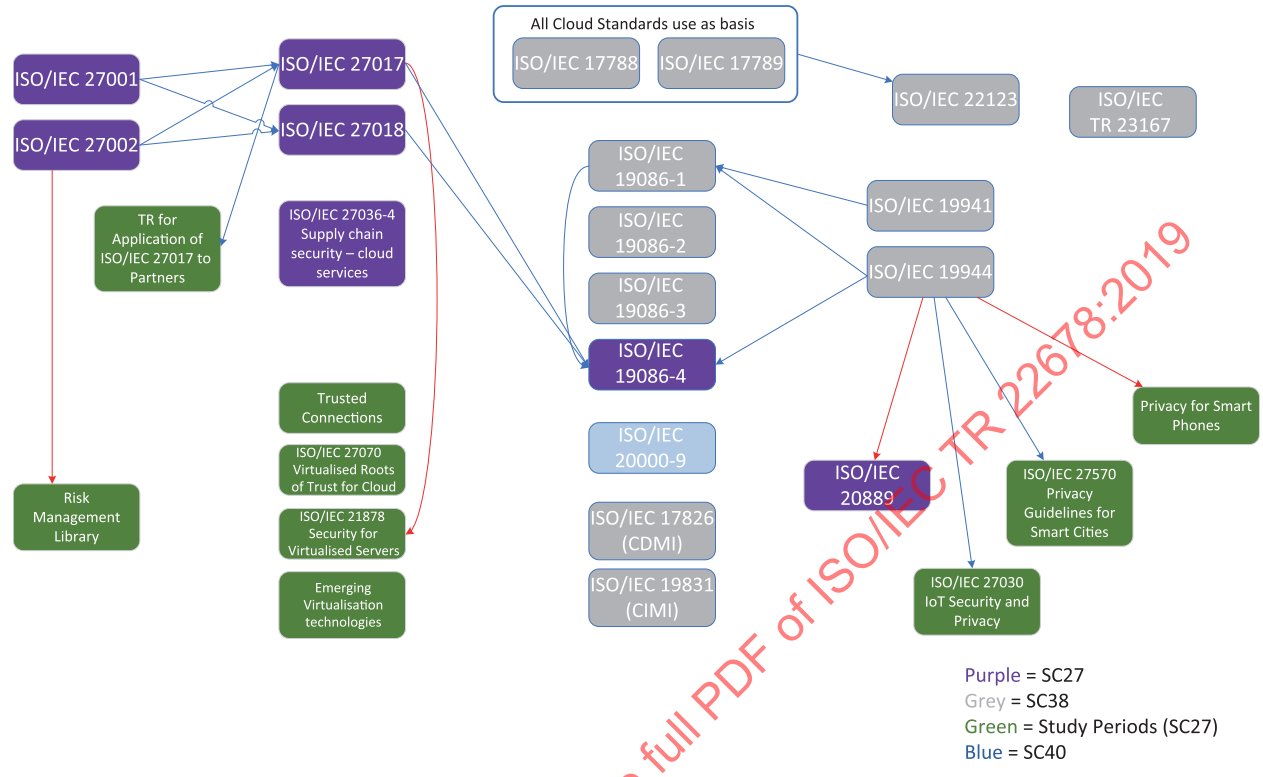


Figure 1 — International standards for cloud computing

NOTE ISO/IEC 27070 is under development (current stage: 10.99), ISO/IEC 27030 is under development (current stage: 20.00), ISO/IEC 27570 is under development (current stage: 20.00).

The following table provides a short description of each of the standards shown in Figure 1.

Standard	Description
ISO/IEC 17788:2014 *Information technology — Cloud computing — Overview and vocabulary*	Provides an overview of cloud computing along with a set of terms and definitions. It is a terminology foundation for cloud computing standards.
ISO/IEC 17789:2014 *Information technology — Cloud computing — Reference architecture*	Specifies the cloud computing reference architecture (CCRA). The reference architecture includes the cloud computing roles, cloud computing activities, and the cloud computing functional components and their relationships.
ISO/IEC 19086-1:2016 *Information technology — Cloud computing — Service level agreement (SLA) framework — Part 1: Overview and concepts*	Seeks to establish a set of common cloud SLA building blocks (concepts, terms, definitions, contexts) that can be used to create cloud Service Level Agreements (SLAs).
ISO/IEC 19086-2 *Cloud computing — Service level agreement (SLA) framework — Part 2: Metric model*	Establishes common terminology, defines a model for specifying metrics for Cloud Service Level Agreements (SLAs), and includes applications of the model with examples. ISO/IEC 19086-2 establishes a common terminology and approach for specifying metrics.
ISO/IEC 19086-3:2017 *Information technology — Cloud computing — Service level agreement (SLA) framework — Part 3: Core conformance requirements*	Specifies the core conformance requirements for service level agreements (SLAs) for cloud services based on ISO/IEC 19086-1 and guidance on the core conformance requirements. This document is for the benefit of and use by both cloud service providers and cloud service customers.

Standard	Description
ISO/IEC 19086-4 *Cloud computing — Service level agreement (SLA) framework — Part 4: Security and privacy*	Specifies security and protection of personally identifiable information components, SLOs and SQOs for cloud service level agreements (cloud SLA) including requirements and guidance.
ISO/IEC 19941:2017 *Information technology — Cloud computing — Interoperability and portability*	Specifies cloud computing interoperability and portability types, the relationship and interactions between these two cross-cutting aspects of cloud computing and common terminology and concepts used to discuss interoperability and portability, particularly relating to cloud services.
ISO/IEC 19944:2017 *Information technology — Cloud computing — Cloud services and devices: Data flow, data categories and data use*	Names and describes the categories of data, flows of data between a device and a supporting cloud services, and how to describe the use of different categories of data by the CSP.
ISO/IEC 27001:2013 *Information technology — Security techniques — Information security management systems — Requirements*	Specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organisation. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organisation. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organisations, regardless of type, size or nature.
ISO/IEC 27002:2013 *Information technology — Security techniques — Code of practice for information security controls*	Gives guidelines for organisational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organisation's information security risk environment(s).
ISO/IEC 27017:2015 *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*	Gives guidelines for information security controls applicable to the provision and use of cloud services by providing: — additional implementation guidance for relevant controls specified in ISO/IEC 27002; — additional controls with implementation guidance that specifically relate to cloud services.
ISO/IEC 27018 *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*	Establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.
ISO/IEC 20889 *Privacy enhancing data de-identification techniques*	Provides a description of privacy-enhancing data de-identification techniques, to be used to describe and design de-identification measures in accordance with the privacy principles in ISO/IEC 29100. In particular, this document specifies terminology, a classification of de-identification techniques according to their characteristics, and their applicability for reducing the risk of re-identification.
ISO/IEC 27036-4:2016 *Information technology — Security techniques — Information security for supplier relationships — Part 4: Guidelines for security of cloud services*	Provides cloud service customers and cloud service providers with guidance on a) gaining visibility into the information security risks associated with the use of cloud services and managing those risks effectively, and b) responding to risks specific to the acquisition or provision of cloud services that can have an information security impact on organisations using these services.

7.1.1 ISO/IEC 19086 series of standards as applicable to trust and transparency

The cloud computing standards created in ISO/IEC JTC1 can be seen as relating to each other from the perspective of cloud service level agreements (SLAs). The ISO/IEC 19086 series of standards describes Cloud Service Level Objectives (SLOs) and Cloud Service Quality Objectives (SQOs) that are the components of cloud service agreements. Such SLOs or SQOs are often described by making references to previous cloud computing standards such as ISO/IEC 27018 for topics related to public cloud processors, or ISO/IEC 19944 for data management SLOs or SQOs that need to build on data taxonomies and use statements.

Figure 2 describes how the ISO/IEC 19086 series of standards reference other standards. It is useful to see how various cloud computing standards are associated with each other from the perspective of cloud service agreements.

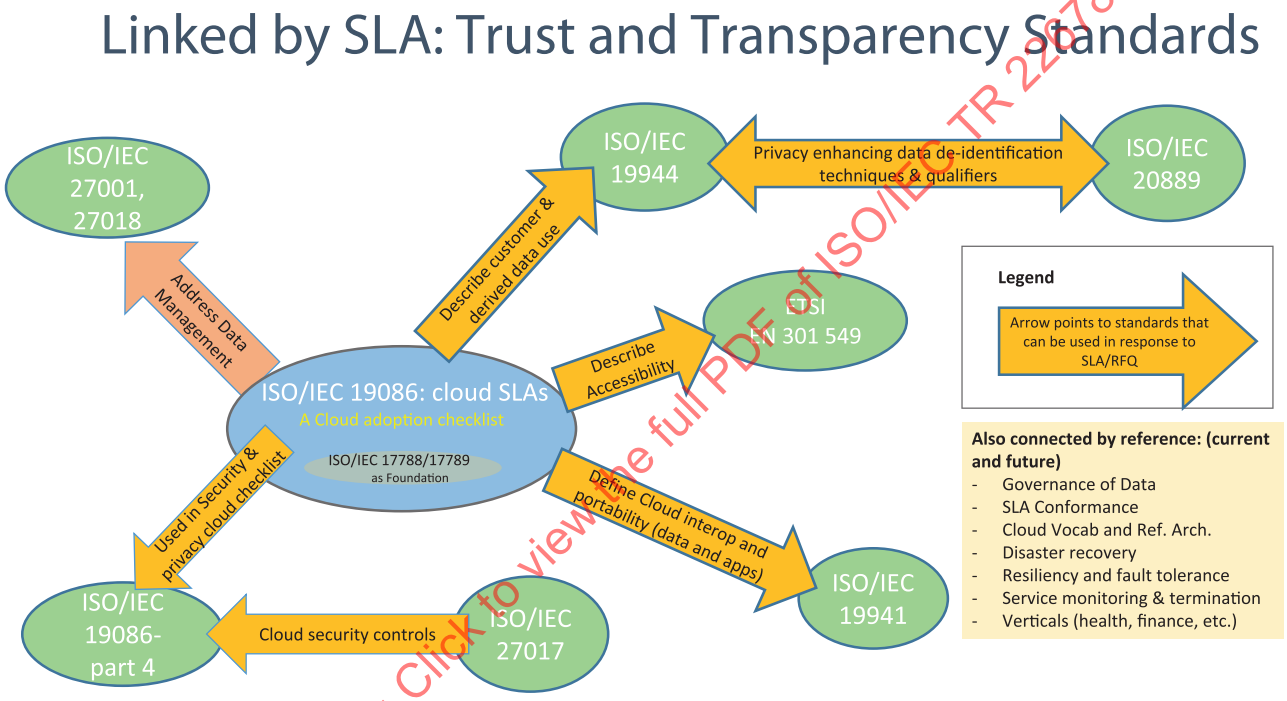


Figure 2 — International standards related to Service Level Agreements (SLOs)

Figure 3 shows a few examples of SQOs that cite other ISO/IEC JTC1 standards such as ISO/IEC 19944 in the areas of data taxonomy and use statements, as well as ISO/IEC 27018 for protection of PII by public cloud operator that act as PII processors. Such use of relevant international standards facilitates the creation of cloud service agreements that are based on internationally recognized consensus concepts and terminologies, allowing for more structured and efficient relationships between cloud service providers, cloud service customers and regulators.

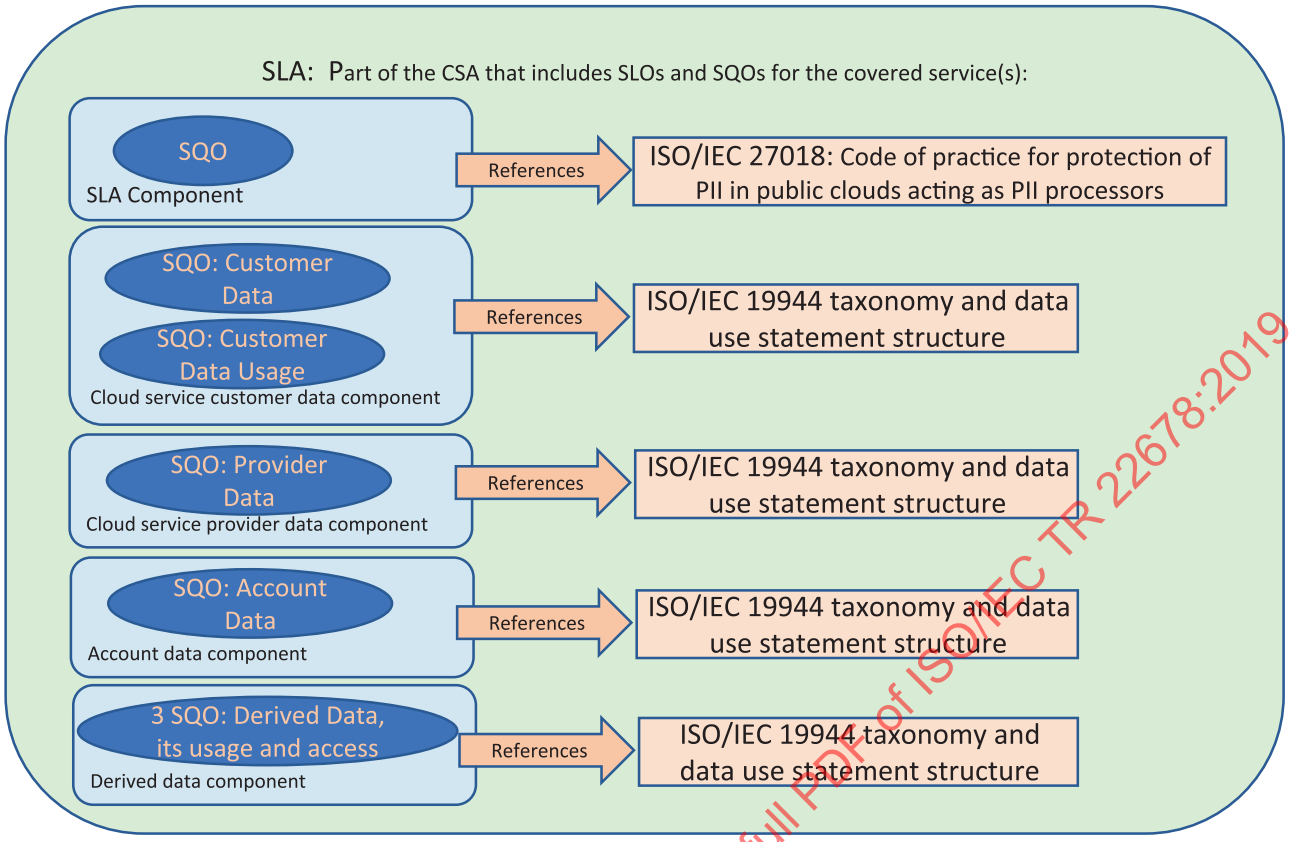


Figure 3 — Examples of SQOs that reference other international standards in the ISO/IEC 19086 series

7.1.2 ISO/IEC 19944 as applicable to clarify data concepts

A similar inter-relationship and dependency map can be established for data-centric standards. At the core is ISO/IEC 19944 that is itself based on foundational cloud computing standards ISO/IEC 17788 and ISO/IEC 17789. ISO/IEC 19944 has been used by other projects in JTC1 such as service level agreements (ISO/IEC 19086 series), de-identification of data (ISO/IEC 20889, data portability (as covered in ISO/IEC 19941).

Understanding this inter-relationship could be useful for public and enterprise policy makers who need to put in place policies and practices using concepts described in them.

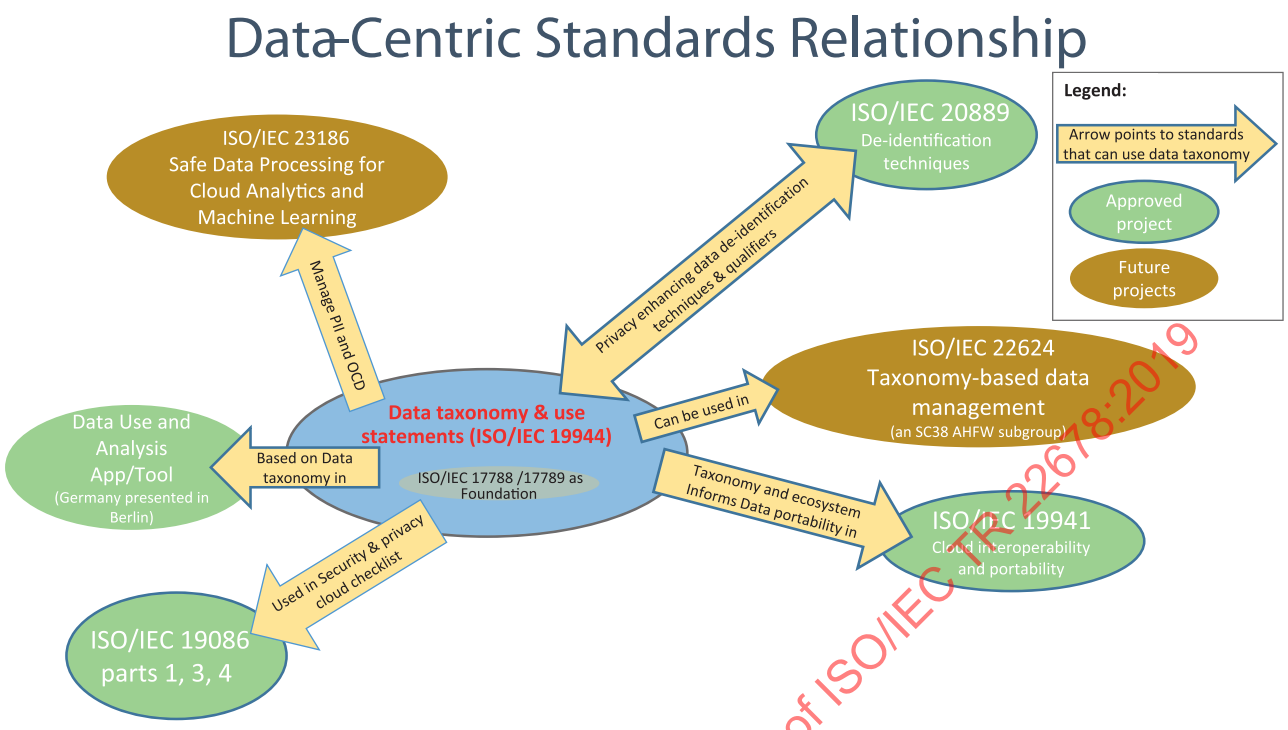


Figure 4 — International standards related to cloud data

7.1.3 ISO/IEC 27552[5], Privacy information management systems

ISO/IEC 27552 is an extension of ISO/IEC 27001 (Information security management systems) as well as ISO/IEC 27002 (Code of practice). In particular, it contains controls suitable for PII controllers and PII processors (that includes cloud computing controllers and processors). ISO/IEC 27552 extends the ISMS by requiring explicitly that PII processing be considered in the scoping of the ISMS, and that privacy be taken into account in terms of interested parties, risks, obligations, etc.

ISO/IEC 27552 is suitable to meet obligations of modern data protection regulations. ISO/IEC 27552 is intended to serve as an assurance mechanism in the controller/processor relationship, as well a generator of evidence that may be useful also for supervisory authorities.

It could also serve as a foundation for privacy information certification, in much the same way that ISO/IEC 27001 and ISO/IEC 27002 serve as a foundation for information security certification.

Figure 5 describes how ISO/IEC 27552 has been derived from the existing international standard for information security management system (ISO/IEC 27001) and how the privacy controls have been developed in relations with, and in composition with security and privacy controls in the existing international standards for codes of practice.

5) Under development. Current stage: 40.00.

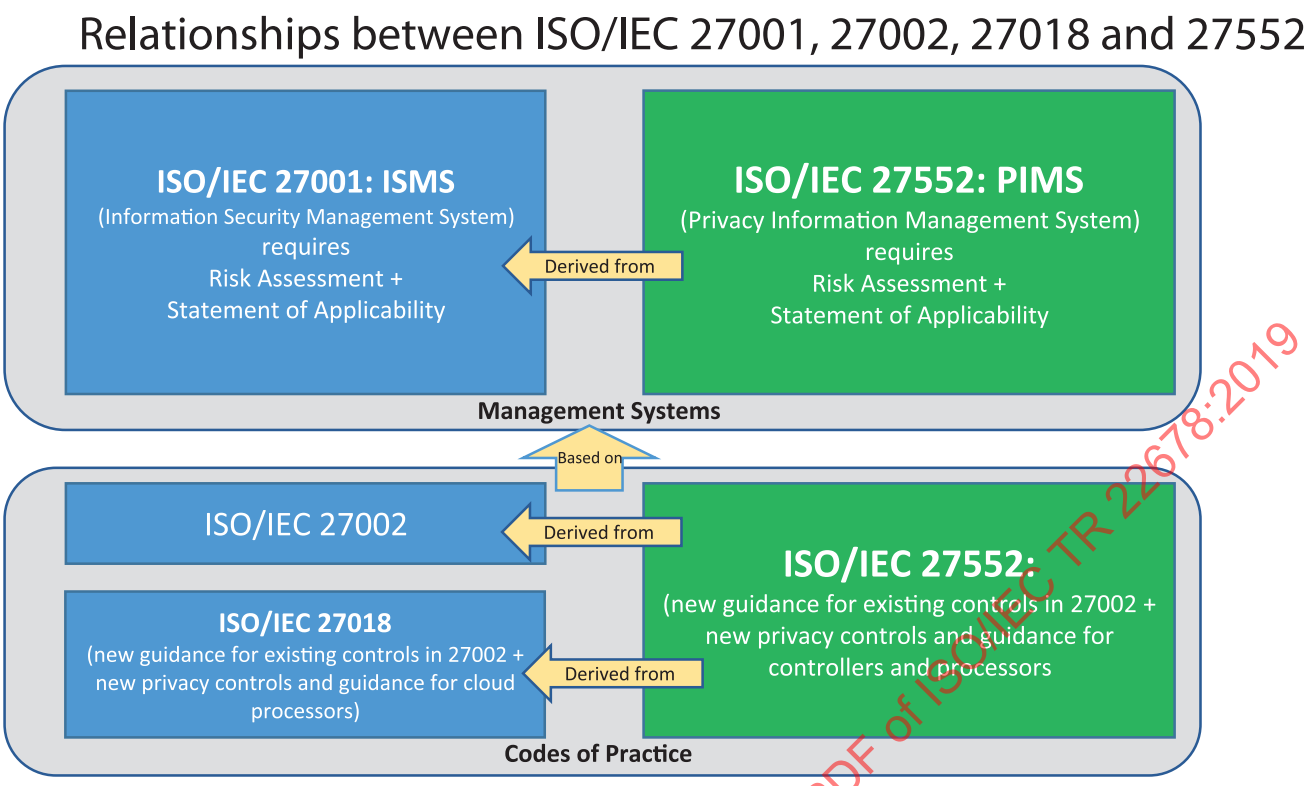


Figure 5 — International standards related to security and privacy in cloud computing

Similar to other ISO/IEC JTC1 standards, ISO/IEC 27552 builds on the existing standards as described in Figure 5 and cites other cloud computing standards such as ISO/IEC 19944 and ISO/IEC 20889 as they contain data taxonomy and data use expressions, as well as de-identification techniques that can be used in privacy-related policy expressions, practices and certifications.

7.2 Other significant standards, specifications, and documents

The cloud computing international standards identified in 7.1 fit within a much wider collection of standards and specifications, many of which may also be useful when developing cloud computing policy. A non-exhaustive list of such additional standards and specifications can be found in Annex B.

8 Considerations when developing policy

8.1 Considerations for regulatory policy

The following are valid considerations when developing policy that will be legally mandated on the deployment, offer, or use of cloud services in a jurisdiction.

The numbering does not imply any form of precedence or priority.

8.1.1 General

CSPs ordinarily provide considerable amounts of documentation to their customers, partners, and regulators. It is therefore unreasonable to diverge from the international consensus on how cloud computing systems are described.

1) Does this policy use or define cloud computing terms in a way that conflicts with the definitions provided in international standards (see 6.2 and ISO/IEC 17788, ISO/IEC 17789)?

2) Does this policy always refer to the international standards for definitions where possible (see 6.2)?

3) Does this policy avoid or mitigate unintended engineering consequences by allowing for reasonable industry consultation before policy changes?

4) Does this policy contain any time constraints and time limits for implementation? Are these consistent with the engineering challenges for implementing the requirements?

8.1.2 Multi-tenant issues

As described in 6.4.7 above, cloud services achieve economy of scale and cost by sharing resources between multiple customers/tenants.

The following for multi-tenant should be considered:

1) Does this policy require that CSPs grant physical access to data or systems by government officials?

    a) If so, how does it protect the rights (e.g. confidentiality, integrity, availability) of other cloud service tenants hosted on the same physical systems or data stores as the target (see 6.4.7)?

2) Does this policy cover deletion of data?

    a) If so, does it take into account the needs of other tenants whose data resides on the same storage media (see 6.4.7)?

3) Does it take into account the financial cost in destroying viable storage media before the end of its working life (see 6.4.3)?

4) Does this policy cover the rights of CSCs to retrieve their data from the CSP?

    a) If so, does this policy take into account the handling of PII about other people that might be embedded within such data?

8.1.3 Avoiding unnecessary barriers to cloud adoption

Policies that were originally developed for regulation of on-premises computing systems or locally hosted systems can sometimes act as obstacles to the deployment of efficient cloud computing architectures.

The following should be considered:

1) Does this policy include implicit assumptions or explicit requirements about CSP staff, such as their citizenship or location (see 6.4.2)?

2) Does the policy require specific local staff qualification(s) or clearance(s) that would make it difficult or impossible to operate or manage by CSP staff based in another jurisdiction (see 6.4.2)?

3) Does this policy constrain the ability of the CSP to move cloud service provider data (see ISO/IEC 19944) between jurisdictions (see 6.4.2, 6.4.3)?

4) Does this policy constrain the storage location of cloud service customer data or derived data to a specific jurisdiction (see 6.4.2)?

    a) If so, does this constraint apply to all such data, or to an identified subset of data categories?

    b) If the latter, are these data categories based on the data taxonomy defined in ISO/IEC 19944?

5) If the policy includes constraints on data location, does it allow for operational exceptions in special circumstances, for example maintaining the cloud service in operation during a major emergency affecting the local cloud datacentre(s)?

6) Is this policy consistent with the international standards for IT governance (see ISO/IEC 38500)?

7) Does this policy allow for continuous development of cloud services and connected applications (see 6.4.6)?

8) Does the policy allow for continuous prototyping, development, test, and deployment?

9) Does the policy encourage or deter CSPs and CSCs keeping their systems up to date?

10) Does the policy require re-certification or re-approval when software is changed?

    a) If so, how much change is permitted before re-certification or re-approval is required?

8.1.4 Trust and transparency

CSCs need to trust their CSP, and experience has shown that trust is best established and maintained by being truthful and transparent about the service(s) being offered, and their operation.

The following should be considered:

1) Does this policy encourage or mandate the use of standards-based terminology in describing online computing services (cloud-based or otherwise)?

2) Does this policy discourage or prohibit the use of terms like "cloud" or "cloud computing" for description of services that don't meet the international standard definition of cloud computing, defined in ISO/IEC 17788 (the practice known as "cloud washing")?

3) Does this policy mandate informing the CSC about how the CSP will make use of customer data or derived data?

    a) If so, does the policy mandate or encourage the CSP making data use statements constructed according to the standard method defined in ISO/IEC 19944?

4) Does this policy require the use of standard terminology in cloud computing service agreements or service level agreements (SLAs)?

    a) If so, does the policy follow the standard terminology and framework defined in ISO/IEC 19086 series?

8.1.5 Interoperability and portability

Interoperability and portability are important issues for CSCs and for regulators, especially for those concerned with competition between service providers. However, this is a very complex subject and needs to be handled carefully.

The following should be considered:

1) Does this policy cover issues of interoperability or portability?

2) Does this policy make clear the distinctions between (see ISO/IEC 19941):

    a) Interoperability

    b) Data portability

    c) Application portability

3) Does this policy mandate specific aspects of interoperability or portability?

    a) If so, are these aspects aligned with or defined using the facets identified in ISO/IEC 19941?

4) Does this policy require direct interoperability (see ISO/IEC 19941), or does it also allow for the use of:

    a) Protocol converters

b) Intermediate formats

c) Third-party data conversion tools (e.g. open source)

d) Other solutions

5) Does this policy require direct data portability, or does it also allow for the use of:

a) Intermediate formats

b) Third-party adapters (e.g. open source)

c) Other solutions

6) Does this policy require direct application portability, or does it also allow for the use of:

a) Emulators

b) Application code conversion

c) Other solutions

8.1.6 Security and privacy

Confidence in information security and the protection of personal information within cloud services is an essential pre-requisite for the successful adoption of cloud computing technologies.

The following should be considered:

1) Does this policy impose specific security requirements on cloud service providers and cloud service customers?

2) Does this policy recognise the concept of shared responsibility between the cloud service provider and the cloud service customer in keeping data secure and private?

3) Does this policy enable and encourage advances in security technology and techniques as new threats emerge?

4) Does this policy enable or promote the use of strong encryption of data at rest and while moving?

5) Does this policy enable the use of industry-trusted risk management approaches to security and privacy such as those described in ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, and ISO/IEC 27552?

8.2 Considerations for advisory policy

8.2.1 General

This subclause covers considerations that are relevant when crafting a policy that advises or recommends on the use of cloud computing but does not impose mandatory requirements.

Examples of such policies would be where a national government provides guidelines and recommendations covering the use of cloud services to local government or to government agencies, though the final decisions of whether (and how) to use cloud services are left to those bodies, such as https://www.gov.uk/government/news/government-adopts-cloud-first-policy-for-public-sector-it.

The following should be considered when developing policy that will provide advice and/or guidance on the deployment, offer, or use of cloud services in a jurisdiction.

The numbering does not imply any form of precedence or priority.

8.2.2 Promotion of cloud technology adoption

Many governments see advantages to business, society and the environment from moving to appropriate cloud computing approaches to IT, as identified in 6.3 above, and will often advise local government and agencies accordingly.

The following should be considered:

1) Does this advisory policy recommend a "cloud first" approach, prioritising the use of public cloud services for those situations where it is technically capable of meeting policy and organisation requirements?

2) Does this policy advise local government or agencies on criteria to determine whether to adopt cloud computing (or not) for their IT needs?

3) Does this policy advise on the environmental benefits of moving to a cloud computing based approach?

8.2.3 Terminology and taxonomy

Correct interpretation of advisory policy depends on common understanding of the terminology used, and correct identification of the categories of data that it will apply to.

The following should be considered:

1) Does this advisory policy use international standard cloud computing terminology according to the defined terms in ISO/IEC 17788 and ISO/IEC 22123?

2) Does this policy only provide general advice or does it provide specific guidance for particular categories or classifications of data (see ISO/IEC 19944), types of application, or purposes?

8.2.4 Adoption by small and medium enterprises

Policies crafted primarily for large scale enterprises and large CSPs can sometimes impose disproportionate burdens on smaller organisations.

The following should be considered:

1) Does this advisory policy assist with or complicate the use of cloud computing for smaller deployments such as small local governments, educational establishments, or smaller agencies?

2) Does this advisory policy encourage or inhibit the adoption of cloud computing by those small and medium enterprises (SMEs) that supply or undertake work for governments and agencies?

8.2.5 Supplier certifications

Following an advisory policy is easier when it provides clear guidance on the type of certifications that can be used to validate full or partial compliance.

The following should be considered:

1) Does this advisory policy give guidance on the type of certifications that might be expected of suppliers and contractors offering cloud-based services to government and agencies?

    a) If so, does this guidance identify suitable certifications against ISO/IEC standards such as those listed in Clause 7?

8.2.6 Network connectivity

Employing cloud computing implies sufficient appropriate network availability, whether via the public Internet or a private network of some kind.

The following should be considered:

1) Does this policy advise on networking issues as essential to cloud computing benefits?

   a) If so, does the policy encourage the provision of sufficient and suitable broadband network connectivity, availability, and reliability?

2) Does this policy provide guidance on appropriate matters of demarcation, such as the scope of responsibilities of CSCs, CSPs (as data controllers and as data processors), and network connection providers?

8.2.7 Interoperability and portability

Enabling interoperability and portability is often cited as essential to free market competition between suppliers of IT services including cloud computing.

The following should be considered:

1) Does this policy provide guidance on the types of interoperability or portability that should be sought?

   a) If so, does the policy adequately articulate the complexity of these topics and follow the international standard framework provided in ISO/IEC 19941?

8.3 Considerations for procurement policy

8.3.1 General

This sub clause covers considerations that are relevant when crafting procurement policies for buyers and users of cloud services, whether purchased by governments, government agencies, or commercial enterprises.

Examples are where a government, enterprise, department, or other CSC sets down rules that will determine, limit or control which cloud services their departments and staff can purchase or employ.

The following should be considered when developing policy that will control the purchase, deployment, offer, or use of cloud services in an organisation.

The numbering does not imply any form of precedence or priority.

8.3.2 Terminology and taxonomy

Some cloud computing and other IT suppliers sometimes use terminology in their marketing or product descriptions which deviates from (or is less clear than) the internationally standardised terms. For a procurement policy, it is important to ensure that the terms used are understood and used in the same way by all suppliers in their service offerings.

The following should be considered:

1) Does this procurement policy use international standard cloud computing terminology according to the defined terms in ISO/IEC 17788, ISO/IEC 22123 and other international standards?

2) Does this procurement policy reference the ISO/IEC 19086 series for cloud service agreement terms and concepts?

3) If this procurement policy places limitations on the use of customer data or derived data by the CSP, does it identify the affected data categories according to the taxonomy described in ISO/IEC 19944?