UNITED NATIONS

Office of Information and Communications Technology

Cloud Computing

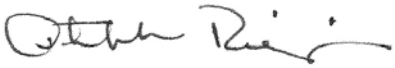
United Nations Secretariat ICT Technical Procedure

REF: INF.09.PROC

Revision History

Serial Number	Release Description	Release Number	Release Date	Author(s)
1	New Document	1.0	17 March 2017	Endorsed by the ICT Policy Committee
2	Revision	2.0	December 2017	Viktorija Kocman, Thomas Braun, Ramzi Hachani, Ramesh Thapa, Gyooshik Choi, Mihai, Valentina, Mark Paat
3	Endorsed by ICT Policy committee	2.1	9 April 2018	Thomas Braun, Gyooshik Choi, Asim Chughtai, Erzen Ilijazi, Evangelos Kokkoris, Ismet Mustafa, John Richards, Jean-Michel Sadoul, Mumtaz Tamim, Kirk Teran
4	Revised and endorsed	2.2	21 March 2019	ICT Policy Committee

Approved By: **Date:**



Atefeh Riazi, ASG/CITO

10 April 2019

Cloud Computing United Nations Secretariat ICT Technical Procedure

Introduction[1]

- **Cloud computing** is a model for enabling ubiquitous, on-demand network access to a shared pool of configurable ICT resources (e.g., networks, servers, storage, applications, and services), that can be rapidly provisioned and released with minimal effort or service provider interaction.

- Cloud Service delivery models:

  There are many different facilities that can be accessed using a cloud architecture including "Infrastructure as a Service" (IaaS), "Platform as a Service (PaaS), and "Software as a Service" (SaaS).

- Cloud deployment models:

  There are four primary cloud computing deployment models which are available to the cloud customer.

1. *Public cloud/external cloud*: This model is publicly accessible and is hosted off-premise. In other words, public cloud is a third-party solution where ICT services are delivered to cloud customers over the Internet.

2. *Private cloud/internal cloud*: This model is managed or owned by an organization and can provide a high level of control over cloud services and infrastructure.

3. *Community model*: A cloud computing environment shared or managed by several related organizations.

4. *Hybrid cloud/virtual private cloud model*: This model, comprised of both private and public clouds, allows for certain components to be hosted by an external party while others remain within the organization's control.

5. *"UN managed cloud"* refers to the public cloud accounts/subscriptions managed by the UN OICT complying to the technical procedure stipulated in this document.

- The United Nations uses the public cloud/external cloud deployment model.

- Cloud computing is playing more of an important role in the modern workplace by providing mission-critical communications, software, infrastructure capabilities and services. However, the inappropriate application or use of cloud computing may represent a huge risk to organizations that can lead to loss of business reputation, security breaches and productivity and/or financial inefficiencies, which may impair the work of the UN.

[1] For more information and concepts related to cloud computing, refer to:
1- "Use of Cloud Computing in the UN System - Recommendations for Risk Mitigation" available on https://iseek.un.org/department/policies
2- NIST Definition of Cloud Computing for definitions of cloud models (IaaS, PaaS, SaaS) and deployment models (public, private, community, hybrid) http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

1 Purpose and Scope

1.1. The purpose of this ICT Technical Procedure is to establish high-level requirements for cloud computing services that are to be consumed by the Secretariat using cloud service providers. It specifies requirements for the acquisition and use of cloud computing services, ensuring that such services meet the UN business, operational, and security needs.

1.2. The objective of this procedure is to mitigate risks that may have an impact on the business continuity and security of United Nations ICT resources and its data. This will also enable financial efficiency and streamline the use of cloud computing at the Secretariat.

1.3. The procedure applies to any organizational entity within the Secretariat that considers using or deploying cloud computing service, regardless of whether it carries a financial cost or not. It applies to all cloud service models (IaaS, PaaS, SaaS) that could be potentially used for the storing, processing, sharing, and/or managing of United Nations ICT data.

1.4. The procedure shall be implemented in accordance with “Organization of the Office of Information and Communications Technology” (ST/SGB/2016/11), “Information Sensitivity, Classification and Handling” (ST/SGB/2007/6), “Use of Cloud Computing in the UN System - Recommendations for Risk Mitigation” (available on https://iseek.un.org/department/policies), and other relevant policies, procedures and Secretariat ICT governance bodies, such as the ICT Architecture Review Board (ICT-ARB), the Software Development Coordination Group (SDCG) and the Project Review Committee (PRC).

2 Definitions

2.1 The following definitions shall apply for the purposes of the present procedure:

a) *ICT service providers*: United Nations Secretariat providers of ICT services to one or more Secretariat entities, defined in ST/SGB/2016/11 as the Office of Information and Communications Technology (OICT), Regional Technology Centres, Enterprise Applications Centres, and Heads of ICT Organizational Units.

b) *Chief Information Technology Officer (CITO)*: The designated Assistant Secretary General who leads and oversees all ICT activities globally and as defined in Section 3 of ST/SGB/2016/11.

c) *ICT resource*: any tangible or intangible asset capable of generating, transmitting, receiving, processing, or representing data in electronic form, where the asset is owned, licensed, operated, managed, or made available by, or otherwise used by, the United Nations.

d) *ICT data*: any data or information, regardless of its form or medium, which is or has been electronically generated by, transmitted via, received by, processed by, or represented in an ICT resource.

e) *Cloud computing*: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources (i.e., servers, operating systems, networks, software, applications, and storage equipment) with self-service provisioning and administration on demand.

f) *Cloud service (CS)*: One or more capabilities offered via cloud computing invoked using a defined interface.

g) *Cloud service administrator*: A person who administers cloud systems contracts as well as ensures cloud computing business and service delivery models are consistently followed and executed within the organization.

h) *Party*: Natural person or legal person, whether or not incorporated, or a group of either.

i) *Cloud service provider (CSP)*: An external party which makes cloud services available.

j) *Cloud service customer (CSC)*: UN Secretariat entity using cloud services.

k) *Cloud service partner (CSN)*: UN ICT service provider which brokers cloud services between the cloud service customer and cloud service provider.

l) *Cloud service-level agreement (C-SLA)*: a contract between a CSP and the Organization that documents what services the CSP will furnish in terms of performance, availability, security, response time, support, etc. It also includes the metrics to measure the services and may include remedies for performance failures, service limitations, and consumer's obligations.

m) *Sensitive information*: ICT data that is classified or the use or distribution of which is otherwise restricted pursuant to applicable administrative issuances. Refer to ST/SGB/2007/6 for details.

3 Overall Responsibility and Accountability

3.1 CSCs are responsible and accountable to review the requirements of this technical procedure and consult with their respective ICT service provider prior to the acquisition and/or use of cloud computing services.

3.2 ICT service providers are responsible and accountable for ensuring the implementation of this technical procedure for any external cloud service that they or their supported clients may acquire, use or provide.

3.3 ICT service providers and CSCs must ensure that a business case has been developed and approved as defined in Section 4, and a C-SLA is formulated in accordance with the requirements defined in 1Appendix 1 of this procedure.

3.4 Following the acquisition of a cloud computing service, ICT service providers are responsible for immediately escalating security related incidents to OICT via established escalation procedures, and taking appropriate containment and mitigation actions, which may include disabling the affected cloud services.

3.5 The CSN is responsible for monitoring the CSP's service levels and for taking actions on deviations.

3.6 OICT shall establish a mechanism for global availability of contracts for acquiring/using external cloud services.

4 General Requirements

Governance

4.1 The acquisition and use of cloud computing services – regardless of cost – must be approved by the CITO and supported by a business case, except for the migration of existing applications and systems to OICT-established enterprise cloud environments. The request for approval shall be routed through the chief of the respective regional technology center (RTC) to the CITO, who will approve/disapprove the request based on the recommendation of the director of the Operations Support Division (OSD) of OICT and the Cloud Service Administrator.

4.2 For all cloud computing services, a business case must be developed by the CSC in collaboration with the responsible ICT service provider, except for the migration of existing applications and systems to OICT-established enterprise cloud environments. The following documentation should be included in the business case:

a) A summary or overview of the intended service including the purpose and benefits of the service, the intended use case in support of the work of the UN, the assessed service criticality, the proposed cloud

service model, key performance metrics for the service and an analysis of the potential security and availability impacts of having the service, which will ensure adherence to organizational standards and enterprise architecture.

b) Intended Data Classification according to ST/SGB/2007/6 (certified by the data owner).

c) A Domain Model (substantive data view) and System Context (identifying all external dependencies).

d) A risk and mitigations assessment (refer to Section on Risk Assessment and Mitigation) addressing the recommendations in the "Use of Cloud Computing in the UN System - Recommendations for Risk Mitigation" available on https://iseek.un.org/department/policies.

e) The analysis of security threats and challenges on the system level, and a list of the high-level security capabilities and security controls that must be in place for the system in question (Appendix 3, available as a separate template).

4.3 The ICT service provider must ensure that the CSP meets the high-level security capabilities that were identified for the system, and that the required security capabilities are reflected in the C-SLA (refer to 1Appendix 1)

Risk Assessment and Mitigation

4.4 The ICT service provider must assess and mitigate the risks associated with the use of its external cloud services. For UN Secretariat entities, the recommendations contained in the "Use of Cloud Computing in the UN System - Recommendations for Risk Mitigation" (available on https://iseek.un.org/department/policies) are mandatory and ICT service providers must follow them to address technical risks.

4.5 CSCs must be involved in the risk assessment and impact analysis, and must approve the final risk assessment and mitigation plan using the signoff template attached to Appendix 3.

Information Security

4.6 The ICT servicer provider must ensure compliance with the confidentiality and disclosure requirements as defined in ST/SGB/2007/6 ("Information Sensitivity, Classification and Handling") as per section 5.4 and ICT security policies (ref: https://iseek.un.org/department/policies) as follows:

4.6.1 The risk assessment of security threats and challenges (Appendix 3) must be performed and included in the business case. Accordingly, mitigation measures and adequate security controls are required depending on the information sensitivity and classification and must be reflected in the C-SLA.

4.6.2 For each system managed in the cloud, a periodic mapping of security threats and challenges to security capabilities must be repeated (updated) by the ICT service provider in collaboration with the CSC (Appendix 3).

4.6.3 A mapping of security threats and challenges to security capabilities must also be repeated after every security breach on CSP infrastructure, upon change of the CSP supply chain, and after every major incident (Appendix 3).

Compliance

4.7 The acquisition and use of cloud computing services must be in compliance with all United Nations regulations and rules including the financial regulations and rules (ST/SGB/2013/4), United Nations ICT policies (https://iseek.un.org/department/policies), enterprise architecture and standards

(https://iseek.un.org/department/standards), and other applicable business and organizational requirements. For instance, the ICT service provider must ensure that the use of the cloud will not adversely impact compliance with the United Nations disaster recovery plans and retention schedules.

4.8 The ICT service provider and the CSC must understand the legal and regulatory requirements concerning the data hosted on the cloud (i.e., disclosure of data to a law enforcement or government agency) in consultation with relevant UN entities (e.g. Office of Legal Affairs (OLA), Procurement Department (PD)), and analyses the potential impact on the privacy and security of ICT data.

5 Ongoing Revisions

5.1 This ICT Technical Procedure must be reviewed by the ICT Policy Committee:

a) on an ongoing basis, at least once every two year;

b) after a major internal security incident has taken place; and

c) following a substantial change to any of the reference Secretary General's Bulletins (SGBs)

Attachments

- **Appendix 1**: Cloud SLAs
- **Appendix 2**: Related Documents
- **Appendix 3**: Security threats and challenges and security capabilities worksheet and signoff template (available as a separated document)

Appendix 1 – Cloud SLA

A cloud service level agreement (Cloud SLA) for cloud services for the United Nations should, at a **minimum**, describe the CSP's capabilities and their related service objective(s) in each of the 33 **core** requirements listed below. These requirements may be listed in documents other than the Cloud SLA (sometime called, Cloud Service Agreement [CSA], Master Service Agreement [MSA], etc.). It is important that the CSC look out for the service objectives offered by the CSC in these other documents.

Core SLA requirements:

- Covered services
- Cloud SLA definitions
- Roles and responsibilities
- Information security
  - Access control
  - Cryptography
- Notification of service termination
- Law enforcement requests
- Governance
  - Regulation adherence
  - Standards adherence
  - Policy adherence
  - Audit schedule
- Availability
- Capacity
- Elasticity
- Service monitoring
- Response time
- Backup methods
- Cloud service support
  - Support plans
  - Support methods
  - Service incident reporting
  - Service incident notification

Each core requirement is described in the tables below. Additionally, the tables below list an additional 66 **important** requirements which the CSC should strongly consider depending on its project's specificities. Finally, there are 26 **optional** requirements the CSC may want to consider, again depending on its project's specificities.

1. Part 1

	Description	Requirement priority
Covered services (9.2)	Identifies the cloud services that are covered by the cloud SLA. All other portions of the cloud SLA apply to the services identified in the covered services component If a single cloud SLA covers multiple services, it could be necessary to provide SLOs and SQOs separately for each covered service	Core
Cloud SLA definitions (9.3)	Includes terms that are unique to the CSP or that are particularly important to the understanding of the agreement. The definitions component is expected to use definitions from industry standards when possible.	Core
Roles and responsibilities (9.5)	Provides a description of roles and responsibilities for both the CSP and the CSC. Cloud computing involves a number of roles, both on the CSC side and also on the CSP side. A clear description of the roles that have relevance to a particular cloud service and the responsibilities of those roles is important for the successful use and operation of the cloud service.	Core

2. Part 2: Organizational cloud service requirements

2.1.Data management

2.1.1. Cloud service provider data

Service (**L**evel/**Q**uality) objective	Description	Requirement priority
(Q) Provider data	A statement defining the cloud service provider data	Important

2.1.2. Cloud service customer data

Service (**L**evel/**Q**uality) objective	Description	Requirement priority
(Q) Cloud service customer data	A statement defining the cloud service customer data, such as the CSC files and database content	Important
(Q) Cloud service customer data usage	A statement of all uses of cloud service customer data by the cloud service provider	Important

2.1.3. Intellectual property rights

Service (**L**evel/**Q**uality) objective	Description	Requirement priority
(Q) Intellectual property rights	A statement of any IPR the CSP claims on the cloud service customer data. Alternatively, or in addition, it is a statement of any IPR the CSP grants to the CSC on the cloud service provider's data and/or cloud service–derived data	Important

2.1.4. Account data

Service (**L**evel/**Q**uality) objective	Description	Requirement priority
(Q) Account data	A statement defining the data elements for account data, such as name, address and telephone	Important

2.1.5. Derived data

Service (**L**evel/**Q**uality) objective	Description	Requirement priority
(Q) Derived data	A statement defining the types of cloud service derived data the CSP creates as a result of interaction with the cloud service by the CSC	Important
(Q) Derived data usage	A statement of all uses of cloud service derived data by the CSP	Important
(Q) Derived data access	A statement describing what access the CSC has to cloud service derived data	Important

2.1.6. Data portability

Service (**L**evel/**Q**uality) objective	Description	Requirement priority
(Q) Data portability capabilities	A statement defining methods, formats and protocols supported by the covered service(s) for the purpose of data portability	Core

2.1.7. Data deletion

Service (**L**evel/**Q**uality) objective	Description	Requirement priority
(L) Data deletion time	A statement describing the maximum time to completely delete cloud service customer	Important

	data including the time for processing the CSC request	
(Q) Data deletion process	A statement of the processes the CSP undertakes to make deleted data irretrievable	Important
(Q) Data deletion notification	A statement describing when and how the CSP will notify the CSC regarding data deletions	Important

2.1.8. Data location

Service (**L**evel/**Q**uality) objective	Description	Requirement priority
(Q) Data location	A statement of what geographic locations the cloud service customer data may be processed and stored in	Important
(Q) Data location specification capability	A statement of whether or not the CSC can specify the geographic locations where their data may be processed and stored	Important
(Q) Data location policy	A list of regulations or policies (internal or external) about Data Location including name, clause and certification number (if applicable), the cloud service provider attests or has been certified to comply with	Important

2.1.9. Data examination

Service (**L**evel/**Q**uality) objective	Description	Requirement priority
(Q) Data examination	A statement of the types of examination the CSP undertakes on cloud service customer data	Important

2.2.Governance

2.2.1. Accessibility

Service (**L**evel/**Q**uality) objective	Description	Requirement priority
(Q) Accessibility standards	A statement listing accessibility related standards the CSP supports in the covered services.	Optional
(Q) Accessibility policies	A statement listing policies and regulations for accessible ICT the CSP supports in the covered services.	Optional

2.2.2. Personally identifiable information

Component	Service (**L**evel/**Q**uality) objective	Description	Requirement priority
Consent and choice (8.1)	(Q) PII principal consent capabilities	A description of the mechanisms provided by the covered services to PII principals to exercise choice and to give consent in relation to the processing of their PII	Important
Purpose legitimacy and specification (8.2)	(Q) Purpose legitimacy	A statement that the CSP only processes PII for purposes explicitly stated in the cloud service agreement A statement that the CSP activities related to PII adhere to appropriate legal, regulatory and contractual requirements.	Important
	(Q) Third party access list	A list of third parties to the agreement between the CSC and the CSP, excluding those listed in response to PII subcontractor list, that have access to PII relating to the CSC, including the CSC's users and tenants.	Important

Data minimization (8.3)	(L) Maximum retention time for temporary files	The maximum period for which temporary files generated during processing are retained before deleted or made permanently inaccessible	Important
	(Q) Minimize stakeholder access	A statement describing the policy for minimizing which people to whom PII is disclosed or have access along with the scope of that access	Important
	(Q) Data minimization cryptographic controls	The description of the cryptographic controls available for minimization of PII processed by the covered services	Important
Use, retention, and disclosure limitation (8.4)	(Q) Data use statements	Statements of the use made by the CSP of any data that could potentially contain PII	Important
Accuracy and quality (8.5)	(Q) PII integrity, accuracy, and quality	A statement describing the policy and process used to check the collected, stored, and updated PII for accuracy, integrity, and quality	Important
Openness, transparency, and notice (8.6)	(Q) PII subcontractor list	A list of the subcontractors of the CSP who have access to the CSC data containing PII	Important
	(Q) Requirement for specific consent	Where the CSP collects PII, a description of the means by which the CSP provides notification to PII principals of the collection, processing and retention of PII and the means by which the CSP obtains and stores their consent	Important

Individual participation and access (8.7)	(Q) PII subject participation and access	Where the CSP collects PII, a statement describing mechanisms by which the CSP supports receiving and responding to complaints, concerns, or questions from PII principals about the CSP's protection of PII practices, including those received directly and through the CSC	Important
	(Q) PII principal access capabilities	The PII principal access capabilities component describes the capabilities available to assist PII principals to exercise their rights to access, correct and erase PII relating to them in the covered services	Important
Accountability (8.8)	(L) PII data breach notification period	Description of the maximum length of time taken for the CSP to notify the CSC of the occurrence of a data breach involving PII	Important
	(Q) Notification of data breach	A statement of the process for notifying a CSC that a data breach has occurred and about the policy the CSP applies in case of a breach of PII data including all procedures and practices followed for incident reporting and remediation	Important
	(Q) PII disposal policy	A description of the policy which the CSP applies to the return, transfer and deletion of PII contained within the cloud service, including any procedures used to make the data inaccessible	Important
Protection of PII compliance (8.9)	(Q) PII processing and storage locations	A list of the geographical locations where PII is stored and processed. Location should include jurisdiction information including country and	Important

		also more specific location information such as city	

2.2.3. Information security

Component	Service (**L**evel/**Q**uality) objective	Description	Requirement priority
Information security policy (7.1)	(Q) Information security policy	A statement that describes the CSP's policies and processes for securing the covered services	Important
Organization of information security (7.2)	(Q) Allocation of roles and responsibilities	A statement of the separation of the roles and responsibilities between the CSP and the CSC	Important
Asset management (7.3)	(L) Asset data update frequency	The maximum interval between refreshes of the asset database	Important
	(Q) Asset and responsibility inventory	A list of the assets or categories of assets and the responsibilities, in terms of the CSC or the CSP, regarding those assets or classes of assets relating to the covered services	Important
Access control (7.4)	(L) Maximum time required to revoke user access	The maximum time required to revoke user access to the covered services	Important
	(L) Time required to revoke user access at a specified commitment level	The time required to revoke user access to the covered services for at least the specified fraction of all such requests	Important
	(Q) User registration and de-registration	A statement describing the process used for registering and de-registering cloud service users for the covered services	Important

	(Q) Review access patterns	A statement describing the capabilities to support review of access patterns and to proactively identify and mitigate potential threats	Important
	(Q) Authentication mechanism	A description of the available authentication mechanisms supported by the CSP on the covered services. A description of the available authentication mechanisms for both users and administrators supported by the CSP on its covered services	Core
	(Q) Third party authentication support	A description of what third party authentication mechanisms are supported by the CSP	Core
	(Q) Strong authentication support	A description of any strong authentication mechanisms which can be used to control CSCs access to covered services. This includes for example multi-factor authentication	Core
	(Q) Anonymous authentication support	A description of available mechanisms for anonymous authentication support provided for the covered services	Core
Cryptography (7.5)	(Q) Cryptographic controls for data in motion	A description of the cryptographic controls available for data in motion associated with the covered services2	Core

[2] These controls provide for securing data with respect to confidentiality and integrity, while being transferred within a covered service, between covered services, and between the CSC and the covered services

	(Q) Cryptographic controls for data at rest	A description of the cryptographic controls available for data at rest associated with the covered services3	Core
	(Q) Cryptographic controls for data during execution	A description of the cryptographic controls available for data during execution associated with the covered services4	Core
	(Q) Key management policy	A statement describing the key management policy for the covered services which may include any mechanisms in place to isolate customer controlled keys from the CSP	Core
Physical and environmental security (7.6)	(Q) Data center monitoring	A statement describing the monitoring done on data centers used for the covered services	Important
	(Q) Secure disposal and re-use of equipment	A description of processes for the secure disposal and re-use of equipment5	Important
	(Q) Facilities authorization	A statement describing the policy and process for granting access to the facilities used to provide the covered services	Important
Operations security (7.7)	(L) Vulnerability reporting interval	The maximum time for the CSP to send a vulnerability report to the CSC following the discovery of a vulnerability	Important

[3] These controls provide for securing data with respect to confidentiality and integrity, while being stored in a covered service
[4] These controls provide for securing data with respect to confidentiality and integrity, while being processed in a covered service
[5] The secure disposal and re-use of equipment process shall ensure that data is deleted from storage devices, and state how devices no longer in use are disposed of

	(L) Period of time of logs availability	A defined period of time during which the logs are available for analysis by the CSC	Important
	(Q) Malware protection	A statement describing mechanisms to ensure the availability and any routine application of any anti-malware protection offered by the CSP for the covered services	Important
	(Q) Logging and monitoring	A statement describing the logging and monitoring relating to the security of the covered services and the methods the CSC can use to access reports of that logging and monitoring	Important
	(Q) Vulnerability management	A description of the process for the monitoring, identification, notification and patching of technical vulnerabilities of the covered services	Important
	(Q) Vulnerability notification method	A description of the method the CSP uses to notify the CSC of technical vulnerabilities and their associated fixes relating to the covered services	Important
	(Q) Vulnerability impact statement	A statement describing the process used by the CSP to describe the impact of vulnerabilities	Important
Communications security (7.8)	(Q) Network segregation	A description of the technical means used to ensure segregation of network access both between tenants in a multi-tenant environment and also between the CSP administration capabilities and the CSC's environment and	Important

		prevent unauthorized tenant to tenant communications	
Systems acquisition, development, and maintenance (7.9)	(Q) System acquisition procedures	A statement that describes the information security related procedures of the CSP when acquiring systems or components from third parties to be used for the provision of the covered services	Important
	(Q) Secure development procedures	A description of the secure development procedures used by the CSP when developing the covered services and associated systems	Important
	(Q) Maintenance procedures	A statement describing the information security and privacy related measures a CSP undertakes to maintain the secure operation of the covered services. Examples are procedures on updating software and hardware, the secure disposal of decommissioned hardware, including the documentation of those steps	Important
Supplier relationship management (7.10)	(Q) Supplier relationship management	A description on how the CSP procures, utilizes, secures, monitors, maintains and reviews the use of third-party services	Important
Information security incident management (7.11)	(L) Information security incident notification period	Description of the maximum length of time taken for the CSP to notify the CSC of the occurrence of an information security incident	Important
	(Q) Information security incident management	A statement documenting information security incident	Important

		management procedures used by the CSP	
Business continuity (7.12)	(Q) Business continuity process	A statement describing the process used by the CSP to ensure business continuity of the cloud service	Important

2.2.4. Termination of service

Service (**L**evel/**Q**uality) objective	Description	Requirement priority
(L) Data retention period	The period of time that cloud service customer data is retained after a notification of service termination has been issued	Core
(L) Log retention period	The period of time that cloud service customer–related log files are retained after a notification of service termination has been issued	Core
(Q) Notification of service termination	A statement of the process for notifying a CSC that their cloud service agreement is being terminated including the notification period	Core
(Q) Return of assets	A statement stipulating responsibilities of the CSP and the CSC in relation to the ownership, use, return and disposal of data objects and the disposal of physical artifacts containing data objects as part of the service termination process	Core

2.2.5. Law enforcement access

Service (**L**evel/**Q**uality) objective	Description	Requirement priority
(Q) Law enforcement requests	A statement of the CSP's plan for notifying CSCs of any law enforcement requests for cloud service customer data or account data	Core

2.2.6. Attestations, certifications, and audits

Component	Service (**L**evel/**Q**uality) objective	Description	Requirement priority
Attestations, certifications, and audit (10.13)	(Q) Cloud service attestations	A list of standards, policies and regulations the CSP attests compliance with or without any third-party verification	Optional
	(Q) Cloud service certifications	A list of standards, policies and regulations where the CSP's compliance has been verified by an accredited certifying body	Optional
	(Q) Cloud service audits	A list of audits the CSP has undertaken with either internal or external resources A list of CSC auditing activities that the CSP can assist with	Optional
Governance (10.9)	(Q) Regulation adherence	A list of regulations including name, clause and certification number (if applicable) the CSP attests or has been certified to comply with	Core
	(Q) Standards adherence	A list of industry standards including name, clause and certification number (if applicable) the CSP attests or	Core

		has been certified to comply with	
	(Q) Policy adherence	A statement to the stakeholders that the business or governance policies specific to the service are being adhered to on an ongoing basis	Core
	(Q) Audit schedule	A schedule of audits the CSP undertakes using its own or third-party resources including the schedule for each audit	Core

3. Part 3: Project cloud requirements

3.1.Performance

3.1.1. Availability

Service (**L**evel/**Q**uality) objective	Description	Requirement priority
(L) Availability	The amount or percentage of time in a given period that the cloud service is accessible and usable[6]	Core

3.1.2. Capacity

Service (**L**evel/**Q**uality) objective	Description	Requirement priority
(L) Limit of simultaneous cloud service connections	Maximum number of simultaneous connections supported by the cloud service	Core
(L) Limit of available cloud service resources	Maximum capacity of available resources, i.e. disk space, CPU power, memory size, page view, etc.	Core

[6] Availability may be calculated as the total time over a set of defined intervals less the total downtime during each interval, and may exclude allowable downtime

(L) Cloud service throughput	The number of inputs or the amount of sets of inter-dependent inputs (i.e. a transaction) that can be processed in every unit of time by the cloud service. It is normally measured as web requests per second, page elements per second and transactions per second	Core
(L) Cloud service bandwidth	The amount of data that can be transferred over a period of time	Core

3.1.3. Elasticity

Component	Service (**L**evel/**Q**uality) objective	Description	Requirement priority
Elasticity (10.4.4)	(L) Elasticity speed	The elasticity speed quantity describes how fast a cloud service is able to react to a resource request when the CSC makes a resource re-allocation request (in the case of manual elasticity), or workload changes take place (in the case of automatic elasticity)	Core
	(L) Elasticity precision	The elasticity precision quantity describes how precise the resource allocation meets the actual resource requirements at a given point in time. In the manual case, precision depends on the granularity of the resource allocation, i.e. the minimum amount of resources that can be re-allocated. Hence, in the manual case, precision is a technical characteristic of the cloud service that does not	Core

		require measurements (i.e. no metric is associated with it) In the automatic case, precision refers to the difference between the amount of resources that are allocated and the amount of resources that are actually needed (the optimum state) to cope with a given workload. The actual resource allocation may be over-provisioned (i.e. more resources are allocated than are actually needed), or under-provisioned (i.e. the amount of resources that are actually allocated is not sufficient to cope with the actual workload). As opposed to the manual case, in the automatic case, the difference between the allocated and the actually needed amount of resources can be determined by a measurement process and hence imply a metric	

3.2.Service

3.2.1. Service monitoring

Service (**L**evel/**Q**uality) objective	Description	Requirement priority
(Q) Monitoring parameters	A list of parameters for the covered services that the CSP monitors and the data is provided to the CSC	Core
(Q) Monitoring mechanisms	A list of mechanisms available to the CSC, such as logs, that includes a description of the monitored parameters and a description of any terms and conditions governing the availability of these mechanisms	Core

3.2.2. Response time

Service (**L**evel/**Q**uality) objective	Description	Requirement priority
(L) Cloud service maximum response time observation	The maximum time between a defined stimulus or input to the cloud service and a defined point in the response	Core
(L) Cloud service response time mean	Statistical mean over a set of cloud service response time observations[7]	Core
(L) Cloud service response time variance	Statistical variance describes how far from the mean response times are likely to be within a set of cloud service response time observations[8]	Core

3.2.3. Service resilience / fault tolerance

Service (**L**evel/**Q**uality) objective	Description	Requirement priority
(L) Time to service recovery	The Time to Service Recovery is the time elapsed between a cloud service failing and the service returning back to the normal state of operation	Important
(L) Mean time to service recovery	The average of a series of Time to Service Restoration calculations[9]	Important
(L) Maximum time to service recovery	The largest value of a set of Time to Service Restoration calculations over a defined period of time	Important
(L) Number of service failures	The number of service failures in total or over a defined period of time	Important

[7] The specification of the method of calculating the mean is defined for metrics associated with the cloud service
[8] Variance is often described in terms of the standard deviation from the mean value of a set of measurements
[9] Mean time to service recovery is inclusive of the hardware-related Mean time to repair service level objective, but in a cloud service environment, hardware is typically virtualized and so the relationship between the time to repair hardware and its impact on service availability is not direct

(Q) Cloud service resiliency/fault tolerance methods	A statement of the methods employed by the cloud service provider which afford resilience and fault tolerance for the cloud service(s) and a statement of the methods available to the cloud service customer to afford resilience/fault tolerance for their own workloads	Important

3.2.4. Backup and restore

Service (**L**evel/**Q**uality) objective	Description	Requirement priority
(L) Backup interval	The period of time between data backups or the number of data backups made in a defined period of time	Optional
(L) Retention period for backup data	The time period the CSP retains data backups	Important
(L) Number of backup generations	The number of backup generations of cloud service customer data retained by the CSP	Optional
(L) Backup restoration testing	The number of restoration tests from backups over a specified time period	Optional
(Q) Backup method	A list of cloud service customer data backup methods available to the CSC or employed by the CSP	Core
(Q) Backup verification	A list of methods or technologies to verify the integrity of data backups	Optional
(Q) Backup restoration test reporting	A statement describing the content and availability of reports on backup restoration testing	Optional
(Q) Alternative methods for data recovery	A list of methods the CSP can undertake to restore cloud service customer data in the	Optional

	event the primary data restoration method is not successful	
(Q) Data backup storage location	List of geographical location(s) where the data backups are stored	Optional

3.2.5. Disaster recovery

Service (**L**evel/**Q**uality) objective	Description	Requirement priority
(L) Recovery time objective	The maximum time period required to bring the cloud service back from an outage to a correct operational state[10]	Important
(L) Recovery point objective	The maximum time period prior to a failure or disaster during which changes to data may be lost as a consequence of recovery[11]	Important
(Q) Cloud service provider disaster recovery plan	A plan that includes a documented set of procedures adopted by the CSP for restoring the cloud service as well as the CSC's applications and data. These procedures can be executed automatically or manually[12]	Important

3.2.6. Cloud service support

Service (**L**evel/**Q**uality) objective	Description	Requirement priority

[10] RTO time period starts when the CSP agrees to initiate recovery process in response to a disaster declared by the CSP and ends when the CSC can resume production operation in the standby/secondary environment. If the decision to fail over is made during a planned downtime, the RTO extends to include the time required to complete the planned maintenance activity by CSP. RTO and RPO do not generally apply to CSC customizations that depend on non-standard components or third-party software

[11] - RPO does not specify the amount of acceptable data loss, only the acceptable amount of time. In particular, RPO affects data redundancy and backup
- Data changes preceding the failure or disaster by at least this time period are preserved by recovery. Zero is a valid value and is equivalent to a "zero data loss" requirement

[12] The RTO and RPO SLOs can form part of the cloud service provider disaster recovery plan

(L) Support hours	The hours of operation for each support plan	Optional
(L) Service incident support hours	The hours during which CSCs may obtain support specifically for service incidents	Optional
(L) Service incident notification time	The time interval in which the CSP will provide a notification of a service incident to specified contacts at the CSC when provided for in the support plan	Optional
(L) Maximum first response time	The maximum time between a customer reporting an incident and the cloud service provider's initial response to the report	Optional
(L) Maximum incident resolution time	States the maximum time for resolving an incident	Optional
(Q) Support plans	A list of the service support plans available to CSCs, including any support costs	Core
(Q) Support methods	Lists the methods the CSC can use to obtain support	Core
(Q) Support contacts	Lists specific contacts for service support if available under the support plan	Optional
(Q) Service incident reporting	Lists the options which the CSC may use to report service incidents to the CSP	Core
(Q) Service incident notification	Lists the terms and conditions (severity, timeframe, etc.) under which the CSP will disclose the details of a service outage or condition that affects the operation of the service. The term may also define what constitutes a service incident.	Core

	The Service Incident Notification may include the cause of the incident, the steps the CSP is taking to resolve the incident, the time at which the CSP expects to have the incident resolved, and any workarounds the CSC may employ while the incident is being resolved.	

Appendix 2 – Related Documents

Related Policies and Guidelines

1. Use of Cloud Computing in the UN System - Recommendations for Risk Mitigation (available on iSeek https://iseek-newyork.un.org/department/policies)
2. Organization of the Office of Information and Communications Technology, ST/SGB/2016/11
3. Information Sensitivity, Classification and Handling, ST/SGB/2007/6
4. Retention Schedule for ICT Records (available on iSeek https://iseek-newyork.un.org/department/policies)
5. Disaster Recovery Planning (available on iSeek https://iseek-newyork.un.org/department/policies)

Other references

1. The NIST Definition of Cloud Computing http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
2. NIST cloud computing standards roadmap http://www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf
3. Cloud Computing Synopsis and Recommendations http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf
4. Guidelines on security and privacy in public cloud computing http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf
5. NIST Cloud Computing Reference Architecture http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505