Vocabulary

December 2016

(**CSP-01-06), Issue-1**

STQC Directorate,
Ministry of Electronics & Information Technology,
Electronics Niketan, 6 CGO Complex, Lodi Road,
New Delhi – 110003.

Accessibility
Usability of a product, service, environment or facility by people within the widest range of capabilities
Note 1 to entry: The concept of accessibility addresses the full range of user capabilities and is not limited to users who are formally recognized as having disability.

Note 2 to entry: The usability-oriented concept of accessibility aims to 33 achieve levels of effectiveness, efficiency and satisfaction that are as high as possible considering the specified context of use, while paying attention to the full range of capabilities within the user population.

Note 3 to entry: It is important in the context of ISO/IEC 19086 to distinguish between the specialized meaning of “accessibility” as defined here and the term “accessible” which is used with its dictionary meaning of “able to be reached or entered”.

Cloud service agreement
Documented agreement between the cloud service provider and cloud service customer that governs the covered service(s)
Note 1 to entry: A cloud service agreement can consist of one or more parts recorded in one or more Documents.

Failure notification policy
Policy specifying the processes by which the cloud service customer and cloud service partner can notify the cloud service provider of a service outage and by which the cloud service provider can notify the cloud service customer and cloud service partner that a service outage has occurred

Note 1 to entry: The policy may also include the process for providing updates on service outages, who receives notifications and updates, the maximum time between the detection of a service outage and the issuance of a notice of service outage, the maximum time interval between service outage updates and how service outage updates are described.

Remedy
Compensation available to the cloud service customer in the event the cloud service provider fails to meet a specified cloud service level objective

Resilience
Ability of a cloud service to recover operational condition quickly after a fault occurs.

Cloud service level objective (SLO)
Commitment a cloud service provider makes for a specific, quantitative characteristic of a cloud service, where the value follows the interval or ratio scale.
Note 1 to entry: an SLO commitment may be expressed as a range.
.
Cloud service qualitative objective (SQO)
Commitment a cloud service provider makes for a specific, qualitative characteristic of a cloud service, where the value follows the nominal or ordinal scale.
Note 1 to entry: a cloud service qualitative objective may be expressed as an enumerated list.
Note 2 to entry: qualitative characteristics typically require human interpretation.
Note 3 to entry: The ordinal scale allows for existence/nonexistence.

Metric

A standard of measurement that defines the conditions and the rules for performing the measurement and for understanding the results of a measurement

Note 1 to entry: A metric implements a particular abstract metric concept.
Note 2 to entry: A metric is to be applied in practice within a given context that requires specific properties to be measured, at a given time(s) for a specific goal.

Disaster recovery
Ability of the ICT elements of an organization to support its critical business functions to an acceptable level within a predetermined period of time following a disaster.

Personally identifiable information (PII)
any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal.

Note to entry: To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to identify that natural person.

PII processor
Privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller

Service level agreement (SLA)
Part of the cloud service agreement that includes cloud service level objectives and cloud service qualitative objectives for the covered service(s).

Business continuity
Capability of the organization to continue delivery of products or services at acceptable predefined levels following disruptive incident

PII controller
Privacy stakeholder (or a privacy stakeholder) that determine the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes.

PII principal
Natural person to whom the personally identifiable information (PII) relates.

Nominal scales
Scale with unordered labelled categories or ordered by convention.

Ordinal scales
Scale with ordered labelled categories.

Interval scale
Continuous scale or discrete scale with equal sized scale values and an arbitrary zero

Ratio scale
Continuous scale with equal sized scale values and an absolute or natural zero point

Data breach
Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed.

Personally identifiable information (PII)
Any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal.

PII controller
Privacy stakeholder (or a privacy stakeholder) that determines the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes

PII principal
Natural person to whom the personally identifiable information (PII) relates

PII processor
Privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller

Processing of PII
Operation or set of operations performed upon personally identifiable information (PII)

Public cloud service provider
Party which makes cloud services available according to the public cloud model

Acceptable use policy
Policy that sets expectations for employees, contractors, and other third parties using Cloud Service
Provider's internal computing resources on the allowed and prohibited activities.

Application account
Account that does not belong to a specific individual that is used to execute programs or services in the background or foreground of the system.

Auditable entities
Auditable entities can be companies, subsidiaries, third parties etc. which are identified based on the scope of the audits.

Cloud computing
Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction as specified in *NIST SP800-145 The NIST Definition of Cloud Computing.*

Cloud environment
Collection of computing resources that cloud users can access or use over a network

Cloud user
A person, organisation or entity that uses services from Cloud Service Providers

Cloud service provider
Organisation responsible for making cloud services available to cloud users

Compliance risk
The risks arising from violations of or non-conformance with official requirements

Cloud service delivery network
Computing resources available to cloud users to host their data or applications

Cloud service management network
The segment of network that is used for performing administrative and maintenance tasks on the Cloud Service Delivery Network

Cloud service provider internal network
The segment of network that is used for internal business processes and not related to providing cloud services

Common vulnerability scoring system (CVSS)
Framework for weighing risks posed by identified vulnerabilities.

Critical network infrastructure
Network devices that support cloud operations. For example, firewall, router, managed switches, load balancers, etc.

Data value
Data value refers to whether the loss, disclosure, or tampering of the data has an adverse impact.

Governance
The process of establishing and maintaining a framework for providing management oversight of an organization's policies, processes, and activities

Hypervisor
Software responsible for managing the flow of information between a virtual operating system and the underlying hardware

Information security policy
Formal document that provides an overview of the security requirements for an organisation-wide information security programme and describes the programme management controls and common controls in place or planned for meeting those requirements

Information security activities
Actions taken to protect the confidentiality, integrity and availability of an organization's information and information assets from unauthorized access, use, modification, insertion, deletion, substitution, destruction, or disclosure.

Information security liaisons (ISL)
ISL serve as points of contact in the organisation, as well as interfacing with external parties for all matters relating to information security. An ISL coordinates with the Information Security management to implement the information security policies, procedures and awareness efforts in the organisation.

Information system
A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information

Isolation
Logical and physical separation of information systems (including data, applications, virtual machines), physical hardware, network traffic, and users in the cloud from threats, vulnerabilities and unauthorized access, as well as restriction of unwanted changes by Cloud Service Provider that could compromise existing security processes.

Key rotation
Process for periodically replacing an encryption key due to expiration or revocation

Non-console access
Access to a system by any means other than direct, local, dedicated cables; e.g. via a network connection, a remote Out Of Band access or any form of wireless connection.

Production data
Data in the cloud environment that has been designated as production data implicitly or explicitly by the cloud user, contract or other formal mechanism. Alternatively, data that is not explicitly referred to as test, development, or another type of non-production data.

Risk management
The process of managing risks through three processes (i) risk assessment; (ii) risk mitigation; and (iii) continuous evaluation

Recovery point objective (RPO)
Point in time to which data shall be recovered after a disruption has occurred as specified in *TR 31:2012 Technical Reference for Security and Service Level Guidelines for the Usage Public Cloud Computing Services*.

Recovery time objective (RTO)
Period of time within which minimum levels of services and / or products and the supporting systems, applications, or functions shall be recovered after a disruption has occurred as specified in *TR 31:2012 Technical Reference for Security and Service Level Guidelines for the Usage Public Cloud Computing Services*.

Self-service portal
A web portal providing self-service for users to access information and perform routine tasks (e.g. provisioning, de-provisioning and managing of resources) over the Internet, without any interaction with system administrators or operators.

Service account
See Application account.

Third party
A person, organisation or entity engaged by the Cloud Service Provider that supports the cloud environment.

Virtualization
Abstraction of physical resources from software

Virtual network
Network implemented within a physical host for VM-to-VM (virtual machine) communication through virtual switches.

Capability
Quality of being able to perform a given activity

Data breach
Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored, or otherwise processed.

Secure multi-tenancy
Type of multi-tenancy that employs security controls to explicitly guard against data breaches and provides validation of these controls for proper governance
NOTE 1 – Secure multi-tenancy exists when the risk profile of an individual tenant is no greater than it would be in a dedicated, single-tenant environment.
NOTE 2 – In very secure environments, even the identity of the tenants is kept secret.

Machine
The complete environment that supports the execution of guest software

Abstract Metric
An abstract standard of measurement used to assess a property. The standard of measurement describes what the result of the measurement means, but not how the measurement was performed. The Abstract Metric is not used by itself, but is instantiated using a Metric.

Abstract Metric Definition
A collection of elements that defines the expression of a specific metric for a given metric category like a blueprint

Cloud Service Property
A property of a cloud service to be observed. A property may be expressed qualitatively or quantitatively.

Concrete Metric Definition
A collection of elements that complete an abstract metric definition by linking the metric to its primary abstract metric and assigning specific values to the rule(s) and parameter(s) defined in the abstract metric definition

Context
The circumstances that form the setting for an event, statement, or idea, in which the meaning of a metric can be fully understood and assessed

Measurement
Set of operations having the object of assigning a Measurement Result.

Measurement Result
Value that expresses a qualitative or quantitative assessment of a property of an entity