Lexicon

A

- ***Anchoring mechanism*** - A channel where solutions to issues are institutionalized through legislation, industry standards, self-governance principles, and other efforts, and which denotes who bears responsibility and liability for implementing them.
- ***Application portability*** - The ability to move executable software from one cloud system to another and be able to run it correctly in the destination system. (Microsoft).

B

- ***Bias*** - Preferential or discriminatory treatment in cloud service availability, deliverability, or functionality.
- ***Brownfield sites*** - Physical land-use properties, such as former gas stations and landfills, that are often difficult to use due to contamination or the presence of hazardous substances. Development of these sites often requires significant investments in pre-development cleanup, revitalization, and monitoring to remain in compliance with local laws. (EPA).

C

- ***Civil rights*** - Personal, social, and political privileges that are protected and enforced by law.
- ***Cloud function*** - The task carried out by a particular cloud service (for example, data processing and storage, security monitoring, and email management).
- ***Cloud incidents*** - Since the word “incidents” is generally understood in the context of cybersecurity (wherein an attack or incidental compromise of systems affects the confidentiality, integrity, and availability of those systems and the data stored, hosted, or processed on them), we have opted to use the phrase “incidents affecting cloud services” to account for other, nonmalicious triggers of failure that can affect cloud services, such as natural disasters.
- ***Cloud service*** - The group of functions under Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Software as a Service (SaaS), as well as other services such as Machine Learning as a Service (MLaaS) and Monitoring as a Service (MaaS).

- ***Cloud service provider (CSP)*** - A company offering some or all types of cloud computing services. Examples include Amazon Web Services (AWS), Microsoft Azure, Google Cloud, IBM Cloud, and Alibaba Cloud.
- ***Cloud market*** - The total market of CSPs and CBSPs, and the system-wide issues that emerge from it.
- ***Cloud-based service provider (CBSP)*** - A company offering a cloud-based service (such as VMware and Salesforce).
- ***Concerns*** - Anxieties, whether real or imagined, of different actors regarding a particular issue. Concerns are often addressed through functional and institutional arrangements aimed at reassuring actors that the problem at hand is indeed being solved.
- ***Consumer cloud*** - Cloud computing services marketed toward individuals and deployed for personal use (for example, Dropbox and iCloud) (Intricately).

D

- ***Data portability*** - The ability to move executable software from one cloud system to another and be able to run it correctly in the destination system. (Microsoft).

E

- ***Enterprise cloud*** - An integrated cloud computational environment that utilizes multiple cloud services (such as PaaS, IaaS, and SaaS) from multiple providers, either public or private.

H

- ***Human rights*** - Inherent and inalienable rights that are bestowed upon all mankind.

I

- ***Infrastructure as a Service (IaaS)*** - Virtualized computing infrastructure resources (for example, application and storage servers and networking) that customers may use according to their needs. Examples include AWS, Azure's Virtual Machine, and Google Compute Engine.
- ***Interoperability*** - The ability of two cloud systems to talk to another, that is, to exchange messages and information in a way that both systems can understand. (Microsoft).

P

- ***Provider-specific*** - Issues or arrangements related to specific CSPs and CBSPs.
- ***Platform as a Service (PaaS)*** - Environments where a customer can use programming tools to develop, run, and manage applications (like Microsoft Azure, Google App Engine, and AWS Elastic Beanstalk).

R

- ***Resilience*** - The ability to recover from foul play or other nonmalicious triggers of failure (like hurricanes, earthquakes, and other natural disasters). May be referred to as "continuity" in other classification schemes.
- ***Robustness*** - The ability to withstand nonmalicious triggers of failure (like hurricanes, earthquakes, and other natural disasters). May be referred to as "resiliency" in other classification schemes.
- ***Risks*** - Pitfalls or potential dangers originating from the technical and operational arrangements that make up the various cloud services. Risks are often addressed through functional and institutional arrangements aimed at preventing or mitigating negative outcomes resulting from each risk.

S

- ***Scope*** - Delineation of the level at which a particular risk, concern, or functional/institutional arrangement applies. Issues can be scoped to the entire cloud market, to specific sectors or providers, to particular functions of specific services, and more.
- ***Sector-specific*** - Topics related to the use of cloud services by specific sectors (especially critical sectors such as power generation, financial services, healthcare, and so on).
- ***Security controls*** - Any safeguards or mechanisms employed to prevent, detect, and minimize security risks to a cloud infrastructure or service.
- ***Software as a Service (SaaS)*** - Applications hosted on the cloud and accessed via a web browser (for example, general business technologies such as email, sales management, and human resource management; popular SaaS applications include Dropbox Office365, Salesforce, and Google Workspace).
- ***Substantive arrangements*** - The methods by which concerns and risks in each issue are addressed (that is, what action is taken to solve the issue).

V

- ***Vital (user) information*** - Information belonging to or generated by a cloud service customer that is considered essential to their usage of the service.