U.S. Treasury
Shared Cloud Lexicon and Terminology

Version July 17, 2024

Contents

Introduction 3
Cloud Computing Terms and Definitions Key 3
Cloud Computing Index 4
Cloud Computing Terms and Definitions 6
Cloud Computing Terms and Definitions Primary Sources 18

Introduction

The Shared Cloud Lexicon and Taxonomy (Lexicon) was created in response to the 2023 US Treasury cloud report, *Adoption of Cloud Services in the Financial Sector*. The Treasury report noted a lack of common definition for terms related to cloud services and technology, critical services, and terms associated with contract negotiation and service level agreements. The report suggested that a shared lexicon and taxonomy, reflecting feedback from financial sector stakeholders, such as the cloud service providers, financial institutions, and regulators, would improve sector communications and the ability to identify critical service dependencies and sector risk.

A representative group of the Financial and Banking Information Infrastructure Committee (FBIIC) member federal agencies (the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Board of Governors of the Federal Reserve System, the Federal Housing Finance Agency and the Securities and Exchange Commission) provided input to US Treasury on development of the Lexicon, which contains terms and definitions from various industry standards and governmental resources. The group then vetted the content with industry stakeholders.

The Lexicon is intended to be beneficial to public and private sector collaboration and communication on cloud-related matters and arrangements. The Lexicon will inform financial sector collaboration and may serve as a shared foundational reference for regulatory agencies, financial institutions, and private sector organizations. The Lexicon includes common risk management and technical terminology with a focus on terms that are often used inconsistently or that have a specific meaning in the context of cloud relationships and services. As cloud computing evolves, as needed, the Lexicon terms and definitions will be updated.

Use of the Lexicon is not required, nor is the Lexicon intended for use in the legal interpretation of any regulations, or regulatory oversight reports or supervisory statements of US financial regulators, international arrangements or agreements, or private contracts. The Lexicon is a product of the US Treasury and represents input from FBIIC member agencies, Financial Services Sector Coordinating Council (FSSCC) members, cloud service providers, and financial sector companies and organizations.

Cloud Computing Terms and Definitions Key

- Definitions for terms that have more than one footnote reference were created by integrating multiple definitions from referenced sources.

- Definitions for terms where the footnote indicates “adapted from” were edited for clarity and not strictly quoted from the referenced sources.

Cloud Computing Index

A

Anything as a Service (XaaS)
Application Program Interface (API)
Availability Zone
API Gateway
Application Stack

B

Blue/Green Deployment

C

Cloud Access Security Broker
Cloud Native Application Protection Platforms
Container
Cloud Broker
Cloud Region
Container Orchestration
Cloud Computing
Cloud Security Posture Management
Content Delivery Network
Cloud Controls Matrix (CCM)
Cloud Service
Continuous Delivery
Cloud Customer
Cloud Service Provider
Continuous Deployment
Cloud Customer Data
Cloud User
Continuous Integration
Cloud Deployment Model
Cloud Workload
Critical Activities
Cloud Infrastructure and Entitlement Management
Cloud Workload Protection Platform (CWPP)
Critical Cloud Services
Cloud Migration
Community Cloud
CSP Data
Cloud Native
Confidential Computing
CSP Derived Data
CSP Partner
CSP Subcontractor

D

Data Lake
Data Security Posture Management
DevSecOps

E

Edge Computing
Enclave

G

Golden Image
Guest Operating System

H

Host Operating System
Hybrid Cloud
Hypervisor

I

Image
Infrastructure as a Service (IaaS)
Infrastructure as Code (IaC)
Instance

L

Load Balancing

M

Measured Service
Microservices
Microservices Architecture
Multi-Cloud
Multi-Tenancy

O

Observability
On-Demand Self Service
Operational Resilience
Orchestrator

P

Platform as a Service (PaaS)
Physical Resource Layer
Portability
Private Cloud
Provisioning/Configuration
Public Cloud

R

Rapid Elasticity
Rapid Provisioning
Redundancy
Resource Abstraction and Control Layer
Resource pooling
Reversibility

S

Scalability
Secure Access Service Edge (SASE)
Secure by Default
Secure by Design
Security Orchestration Automation and Response (SOAR)
Serverless
Service Level Agreement (SLA)
Service Mesh
Service Orchestration
Service-Oriented Architecture (SOA)
Service Provider Concentration (Financial Institution)
Service Provider Concentration (Financial sector)
Service Provider Concentration Risk (Financial Institution)
Service Provider Concentration Risk (Financial Sector)
Shared Responsibility
Software as a Service (SaaS)
Software Bill of Materials (SBOM)
Standard Image
Supply Chain
Supply Chain Risk

T

Tenant

V

Virtualization
Virtual Machine

Cloud Computing Terms and Definitions

Anything as a Service (XaaS) - A services delivery model that summarizes several categories of IT, including those delivered in the cloud as a subscription-based service.[1]

Application Program Interface (API) - Software code and a set of defined rules that enable different applications to communicate with each other. It acts as an intermediary layer that processes data transfers between systems, allowing a cloud customer to access its application data and functionality to external third-party developers, business partners, and internal business units.[2,3]

API Gateway - Software that takes an application user's API request, routes it to one or more backend services, gathers the appropriate data, and delivers it to the user in a single, combined package. It also provides analytics, layers of threat protection, and other security for the application.[4]

Application Stack - A collection of independent components that work together to support the execution of an application. In a cloud environment, the components may include hardware, virtualization (hypervisor), communication protocols (API), guest operating system, service/application, and orchestration.[5]

Availability Zone – Logically and physically isolated data centers that host cloud services. Availability zones are located in a cloud region. The availability zones are usually grouped into regions with the major cloud providers offering multiple regions across the globe.[6,7]

Blue/Green Deployment - A deployment strategy in which two separate, but identical environments are created that can reduce the impact of interruptions caused due to issues in the new version being deployed. This is achieved by exposing the new version of the software to a limited set of users and expanding that user base gradually until everyone is using the new version. If at any time the new version is causing issues all the users can be instantly redirected to the old version. One environment (blue) is running the current application version and one environment (green) is running the new application version.[8,9,10]

---

[1] Adapted from https://www.gartner.com/doc/4547799
[2] Adapted from https://ithandbook.ffiec.gov/glossary/
[3] Adapted from https://www.ibm.com/topics/api#:~:text=the%20next%20step-,What%20is%20an%20API%3F,to%20communicate%20with%20each%20other
[4] https://www.ibm.com/cloud/blog/api-gateway#:~:text=An%20application%20programming%20interface%20(API,in%20a%20single%2C%20combined%20package
[5] Adapted from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-292.pdf
[6] Adapted from https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf
[7] Adapted from https://www.iso.org/obp/ui#iso:std:iso-iec:22123:-1:ed-2:v1:en
[8] Adapted from https://azure.microsoft.com/en-us/blog/blue-green-deployments-using-azure-traffic-manager/
[9] Adapted from https://cloud.google.com/terms/services
[10] Adapted from https://docs.aws.amazon.com/whitepapers/latest/overview-deployment-options/bluegreen-deployments.html

Cloud Access Security Broker (CASB) - A software tool or service that sits between a cloud customer's on-premises infrastructure and a cloud service provider's infrastructure as a "gatekeeper" to monitor activity and enforce the cloud customer's security policies (e.g., authentication, single sign-on, authorization, credential mapping, and encryption) as the cloud-based resources are accessed.[11,12]

Cloud Broker - An entity that manages the use, performance, and delivery of cloud services, and negotiates relationships between cloud service providers and cloud service customers.[13]

Cloud Computing - 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.[14]

Cloud Customer - Entity that contracts with a cloud service provider for the purpose of using cloud services.[15]

Cloud Customer Data - Data under the control of the cloud service customer that were inputted to the cloud service or resulted from exercising the capabilities of the cloud service.[16]

Cloud Deployment Model - Way in which cloud computing can be organized based on the control and sharing of physical or virtual resources (e.g., public, private, hybrid, and community cloud).[17]

Cloud Infrastructure and Entitlement Management (CIEM) – Identity-centric SaaS solutions for managing cloud access risk, including the governance of entitlements and detection of anomalies in hybrid and multi-cloud IaaS.[18]

Cloud Migration - The process of transitioning workloads, applications and data for example from an entity's private, on-premises technology to a cloud service provider's computing environment, or between different cloud environments. [19]

Cloud Native - A software approach of building, deploying, and managing modern applications to leverage or implement cloud characteristics in cloud computing environments.[20, 21]

---

[11] Adapted from https://ithandbook.ffiec.gov/glossary/
[12] Adapted from https://www.gartner.com/en/information-technology/glossary?glossaryletter=C
[13] Adapted from https://csrc.nist.gov/glossary
[14] https://csrc.nist.gov/glossary
[15] Adapted from ISO/IEC 17788 Information Technology Cloud Computing Overview and Vocabulary
[16] Adapted from https://www.iso.org/obp/ui#iso:std:iso-iec:22123:-1:ed-2:v1:en
[17] Adapted from https://www.iso.org/obp/ui#iso:std:iso-iec:22123:-1:ed-2:v1:en
[18] https://orca.security/lp/gartner-innovation-insight-cloud-infrastructure-entitlement-management-ciem/
[19] Adapted from https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-cloud-migration/#definition
[20] Adapted from https://www.gartner.com/en/information-technology/glossary?glossaryletter=C
[21] Adapted from https://aws.amazon.com/what-is/cloud-native/

Cloud Native Application Protection Platforms (CNAPP) – A unified and tightly integrated set of security and compliance capabilities designed to secure and protect cloud-native applications across development and production.[22]

Cloud Region - Geographical area served by a cloud data center that is independent and isolated from other cloud data centers in other geographical areas. Each data center region is intended to be isolated to limit the probability of concurrent disruption.[23]

Cloud Security Posture Management (CSPM) – A service that manages IaaS and PaaS security posture through prevention, detection, and response to cloud infrastructure risks. CSPM applies common frameworks, regulatory requirements, and enterprise policies to discover and assess risk in cloud services configuration and security settings, with remediation options provided.[24]

Cloud Service - Infrastructure, platforms, software, or data storage that are hosted by cloud service providers and made available to cloud service customers through the internet.[25]

Cloud Service Provider (CSP) - A company offering a cloud-based platform, infrastructure, application, or storage services that provides on-demand, scalable computing resources like computing power, data storage, or applications.[26, 27]

CSP Data - Data specific to the operation of the cloud service, under the control of the cloud service provider.[28]

CSP Derived Data - Data under cloud service provider's control that are derived as a result of interaction with the cloud service by the cloud customer.[29]

CSP Partner - A third-party that integrates a software or service with a cloud service provider's system, to support the cloud service provider's or cloud customer's business functions, operations, and cloud services.[30]

CSP Subcontractor - A third party that provides a service to a CSP that supports a CSP's provision of its cloud services to its cloud customers.[31]

Cloud User - Persons to include employees and third parties as designated by the cloud customer to access cloud services.[32]

---

[22] https://www.gartner.com/reviews/market/cloud-native-application-protection-platforms
[23] Adapted from https://www.iso.org/obp/ui#iso:std:iso-iec:22123:-1:ed-2:v1:en
[24] https://www.gartner.com/en/information-technology/glossary/cloud-security-posture-management
[25] Adapted from https://www.redhat.com/en/topics/cloud-computing/what-are-cloud-services
[26] Adapted from https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-cloud-provider/
[27] Adapted from https://cloud.google.com/terms/services
[28] Adapted from https://www.iso.org/obp/ui#iso:std:iso-iec:22123:-1:ed-2:v1:en
[29] Adapted from https://www.iso.org/obp/ui#iso:std:iso-iec:22123:-1:ed-2:v1:en
[30] Adapted from ISO/IEC 17788 Information Technology Cloud Computing Overview and Vocabulary
[31] Google
[32] Adapted from https://www.occ.gov/news-issuances/bulletins/2021/bulletin-2021-36a.pdf

Cloud Workload - A set of customer applications, services, or capabilities that consumes compute, network, storage, or other cloud services.[33]

Cloud Workload Protection Platform (CWPP) – A platform designed to facilitate visibility and management of security controls in cloud and multi-cloud environments.[34]

Community Cloud - A shared cloud computing service environment that is targeted to a limited set of organizations or employees (such as financial institutions or heads of trading firms). The organizing principle for the community will vary, but the members of the community generally share similar security, privacy, performance, and compliance requirements. Community members may invoke a mechanism to manage those seeking entry into the community.[35]

Confidential Computing – Hardware-enabled features that isolate and process encrypted data in memory so that the data is at less risk of exposure and compromise from concurrent workloads or the underlying system and platform.[36]

Container - A construct designed to package and run an application or its components on a shared operating system. Application containers are isolated from other application containers and share the resources of the underlying operating system, allowing for efficient restart, scale-up, or scale-out of applications across clouds. Application containers typically contain microservices.[37]

Container Orchestration – A software tool that automates the provisioning, deployment, networking, scaling, availability, and lifecycle management of containers.[38]

Content Delivery Network - A network of servers that is geographically dispersed to enable faster web performance by locating copies of web content closer to users or facilitating delivery of dynamic content (e.g., live video feeds).[39]

Continuous Delivery - The process of automating software development, testing, configuration, and deployment from a build to a production environment.[40]

Continuous Deployment - Similar to continuous delivery except that the software releases happen automatically without human intervention, and changes to code are available to customers immediately after they are made.[41]

---

[33] https://cloud.ibm.com/docs/overview?topic=overview-glossary
[34] https://www.cisa.gov/sites/default/files/2023-12/CISA%20TIC%203.0%20Cloud%20Use%20Case_508c.pdf
[35] Adapted from https://www.gartner.com/en/information-technology/glossary?glossaryletter=C
[36] https://csrc.nist.gov/glossary/term/confidential_computing
[37] https://csrc.nist.gov/files/pubs/sp/800/180/ipd/docs/sp800-180_draft.pdf
[38] https://www.ibm.com/topics/container-orchestration?mhsrc=ibmsearch_a&mhq=container%20orchestrator
[39] https://www.ibm.com/topics/content-delivery-networks#:~:text=A%20content%20delivery%20network%20is,e.g.%2C%20live%20video%20feeds)
[40] Adapted from https://learn.microsoft.com/en-us/devops/deliver/what-is-continuous-delivery
[41] https://csrc.nist.gov/glossary

Continuous Integration - An integrated set of practices and software tools used to merge developers' code, build, and test the resulting software, and package it for deployment.[42]

Critical Activities – Activities of a financial institution, including associated products, services, operations, systems, functions, and support, that (a) upon failure would result in significant consumer harm or significant loss of revenue, profit, reputation, or franchise value of the financial institution, or (b) the failure or discontinuance of which would pose a threat to the financial stability of the United States.[43]

Critical Cloud Services – Services from a cloud service provider including associated operations, systems, functions, and support, consumed by a financial institution that upon failure or disruption would have a significant, adverse impact on critical activities.

Data Lake - A centralized repository designed to store, process, and secure large amounts of structured, semi structured, and unstructured data. It can store data in its native format and process any variety of it, ignoring size limits. A data lake can store both structured and unstructured data. [44, 45]

Data Security Posture Management - A cybersecurity technology that identifies sensitive data across multiple cloud environments and services, assessing its vulnerability to security threats and regulatory risk.[46]

DevSecOps - A software engineering culture and practice that aims at unifying software development (Dev), security (Sec) and operations (Ops). The main characteristic of DevSecOps is to automate, monitor, and apply security at all phases of the software development life cycle (SDLC).[47]

Edge Computing – A distributed computing framework, bringing information storage and computing abilities closer to the devices that produce that information and the users who consume it. By shifting processing capabilities closer to users and devices, edge computing systems significantly improve application performance, reduce bandwidth requirements, and give faster real-time insights.[48, 49]

[42] https://www.axelos.com/resource-hub/glossary/itil-v3-glossaries-of-terms
[43] Adapted from https://www.federalregister.gov/documents/2021/11/23/2021-25510/computer-security-incident-notification-requirements-for-banking-organizations-and-their-bank
[44] Adapted from https://cloud.google.com/learn/what-is-a-data-lake#:~:text=A%20data%20lake%20is%20a,data%20lake%20on%20Google%20Cloud
[45] Adapted from https://www.ibm.com/topics/data-lake
[46] https://www.ibm.com/topics/data-security-posture-management
[47] Adapted from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-204C.pdf
[48] Adapted from https://aws.amazon.com/what-is/edge-computing/
[49] Adapted from https://www.ibm.com/cloud/what-is-edge-computing

Enclave - A set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter. Enclaves are generally separate, hardened, and highly constrained virtual machines.[50, 51]

Golden Image - Virtual machine (VM) images and container images that go through processes where required patches and updates are applied, security policies are configured, and security applications are installed. Scans are then executed to verify the results of the process and validate whether an image fulfills all appropriate security considerations. Post-creation, these images can then be put into stored repositories and used later to replace running production images. This creation process can be completed on a regular basis so that new images are released monthly, weekly, hourly, or even in response to recently discovered vulnerabilities.[52]

Guest Operating System - A virtual machine that runs an instance of an operating system and its applications.[53]

Host Operating System - The operating system that controls the hardware.[54]

Hybrid Cloud - A composition of two or more clouds (on-site private, on-site community, off-site private, off-site community or public) that remain as distinct entities but are bound together by standardized or proprietary technology that enables data and application portability.[55]

Hypervisor – Software that manages the guest operating systems (OSs) and controls the flow of instructions between the guest OSs, virtual machines, and/or the physical hardware.[56]

Image - A compute resource that stores all the configuration, metadata, permissions, and data from multiple disks of a virtual machine.[57]

Infrastructure as Code (IaC) - The process of managing and provisioning an organization's IT infrastructure using machine-readable configuration files, rather than employing physical hardware configurations or interactive configuration tools.[58]

Infrastructure as a Service (IaaS) – A cloud service model that provides cloud customers with the ability to provision processing, storage, networks, and other fundamental computing resources where the cloud customer is able to deploy and run software, which can include guest operating systems and applications. The cloud customer does not manage or control the

[50] https://csrc.nist.gov/glossary/term/enclave
[51] https://docs.aws.amazon.com/enclaves/latest/user/nitro-enclave.html
[52]https://www.cisa.gov/sites/default/files/publications/Cloud%20Security%20Technical%20Reference%20Architecture.pdf
[53] https://csrc.nist.gov/glossary
[54] Developed by the Cloud Lexicon working group.
[55] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-292.pdf
[56] https://csrc.nist.gov/glossary
[57] Adapted from https://cloud.google.com/terms/services
[58] https://csrc.nist.gov/glossary

underlying cloud infrastructure; however, it has control over operating systems, storage, and deployed applications.[59]

Instance - An instance abstracts physical computing infrastructure using virtual machine technology. It is similar to having a server(s) in the cloud.[60]

Load Balancing - Software or hardware that distributes workloads across multiple computing resources to optimize resource use, avoid overloading any single resource, and direct users to another server if the initial server fails.[61]

Measured Service - Systems that automatically control and optimize resource use by leveraging a metering capability (e.g., storage, processing, bandwidth, and active user accounts) appropriate to the type of service. Resource usage can be monitored, controlled, and reported.[62]

Microservices - A set of containers that work together to compose an application.[63]

Microservices Architecture - A design method that uses basic elements called microservices, each running in its own process and communicating with APIs.[64]

Multi-Cloud – Cloud deployment model in which a cloud customer uses public cloud services provided by two or more cloud service providers. This may involve each CSP supporting different workloads or multiple CSPs supporting the same workloads. [65]

Multi-Tenancy - The mode of operation of software where multiple independent instances of one or more applications operate in a shared environment. The instances (tenants) are logically isolated, but physically integrated.[66]

Observability - The capability to understand and diagnose the internal state of a system by analyzing its external outputs, such as metrics, logs, and traces, enabling issue detection and performance optimization.

On-Demand Self Service - A cloud customer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.[67]

---

[59] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-316.pdf
[60] https://aws.amazon.com/what-is/cloud-instances/#:~:text=A%20cloud%20instance%20abstracts%20physical,in%20the%20cloud%20computing%20environment
[61] https://cloud.ibm.com/docs/overview?topic=overview-glossary
[62] https://csrc.nist.gov/glossary
[63] https://csrc.nist.gov/glossary
[64] Challenges in Securing Application Containers and Microservices : CSA
[65] Adapted from https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf, and https://www.iso.org/obp/ui#iso:std:iso-iec:22123:-1:ed-2:v1:en
[66] https://www.gartner.com/en/information-technology/glossary?glossaryletter=C
[67] https://csrc.nist.gov/glossary

Operational Resilience - Operational resilience is the ability to deliver operations through any disruption. It is the outcome of effective operational risk management combined with sufficient financial and operational resources to prepare, adapt, withstand, and recover from disruptions.[68]

Orchestrator - A tool that enables DevOps personas or automation working on their behalf to pull images from registries, deploy those images into containers, and manage the running containers. Orchestrators are also responsible for monitoring container resource consumption, job execution, and machine health across hosts.[69]

Physical Resource Layer - Includes all the physical resources used to provide cloud services, most notably, the hardware and the facility. The CSP updates and maintains the hardware, network infrastructure, environmental controls, power, physical security, data communications connections.[70, 71]

Platform as a Service (PaaS) - A cloud service model that provides the cloud customer with the capability to deploy onto the cloud infrastructure cloud customer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The cloud customer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.[72]

Portability - The ability to transfer systems and data from one cloud-based system to another.[73]

Private Cloud - Gives a single cloud service customer the exclusive access to and usage of the infrastructure and computational resources. It may be managed either by the cloud customer or by a third party, and it may be hosted on the cloud customer's premises (i.e., on-site private clouds) or outsourced to a hosting company (i.e., outsourced private clouds). In both scenarios, services are not accessible, or even publicly visible, over the internet.[74, 75]

Provisioning/Configuration - The activity of obtaining, modifying, and making available the equipment, resources, software, or services a cloud service customer needs to carry out a particular cloud activity. Depending upon the activity, provisioning can be performed by the cloud service provider or cloud customer.[76]

Public Cloud - Cloud infrastructure and computing resources are made available to the general public. A public cloud is owned by an organization selling cloud services and serves a diverse pool of clients.[77]

---

[68] https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-144a.pdf
[69] https://csrc.nist.gov/glossary
[70] Adapted from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-292.pdf
[71] Adapted from https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf
[72] Adapted from https://csrc.nist.gov/glossary
[73] https://www.iso.org/obp/ui/en/#iso:std:iso-iec:22123:-1:ed-2:v1:en
[74] Adapted from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-292.pdf
[75] Adapted from https://www.fsb.org/wp-content/uploads/P091219-2.pdf
[76] Adapted from https://ithandbook.ffiec.gov/glossary/
[77] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-292.pdf

Rapid Elasticity - Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the cloud customer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.[78]

Rapid Provisioning - Automatically deploying a cloud system based on the requested service/resources/capabilities.[79]

Redundancy - The duplication of components or functions of a system with the intention of increasing reliability.

Resource Abstraction and Control Layer - Software, or software elements, such as hypervisor, virtual machines, virtual data storage, and supporting software components, used to realize the infrastructure upon which a cloud service can be established.[80]

Resource pooling - The provider's computing resources are pooled to serve multiple cloud customers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to cloud customer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.[81]

Reversibility - Process for service provider customers to retrieve their data and application artifacts, and for the service provider to delete all service provider customer data as well as contractually specified service derived data after an agreed period.[82]

Scalability - The measure of a service's capacity to increase or decrease in performance and resources in response to changes in volumes or general computing or network needs.[83]

Secure Access Service Edge (SASE) – Cloud-delivered architecture that securely connects networks, users, systems, endpoints, and remote networks to apps and resources.[84]

Secure by Default – A principle by which technology products are secure to use "out of the box" with little to no configuration changes necessary and contain security features available at no additional cost.[85]

---

[78] Adapted from https://csrc.nist.gov/glossary
[79] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-292.pdf
[80] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-292.pdf
[81] https://csrc.nist.gov/glossary
[82] https://www.iso.org/obp/ui#iso:std:iso-iec:22123:-1:ed-2:v1:en
[83] https://www.fsb.org/wp-content/uploads/P091219-2.pdf
[84] https://www.microsoft.com/en-us/security/business/security-101/what-is-sase
[85] https://www.cisa.gov/securebydesign

Secure by Design – A principle by which technology products are built in a way that reasonably protects against malicious cyber actors successfully gaining access to devices, data, and connected infrastructure.[86]

Serverless - A way to build and run applications and services without having to manage infrastructure. Applications still run-on servers, but all the server management is done by the CSP. The user does not have to provision, scale, and maintain servers to run applications, databases, and storage systems.[87]

Service Level Agreement (SLA) - A contractual agreement between an entity and a service provider that defines service operational topics, such as a party's responsibilities for the level of service, priorities, and guarantees regarding timing, availability, performance, and other key aspects of the service delivered.[88]

Service Mesh - An infrastructure layer in an application that facilitates communication between services. Service meshes provide capabilities like traffic management, resiliency, policy, security, strong identity, and observability to workloads.[89]

Service Orchestration - The composition of system components to support the cloud provider's activities in arrangement, coordination, and management of computing resources in order to provide cloud services to cloud customers.[90]

Security Orchestration Automation and Response (SOAR) - Refers to technologies that enable entities to collect inputs monitored by the security operations team. SOAR tools allow an organization to define incident analysis and response procedures in a digital workflow format.[91]

Service-Oriented Architecture (SOA) - In SOA, the entire gamut of solutions (e.g., supporting a business process) is broken up into multiple parts or components called services. This approach makes the development, maintenance, and deployment of the entire application easier as operations can be limited to a specific service rather than to an entire application.[92]

Service Provider Concentration (Financial Institution) – The extent to which a financial institution relies on a service provider, directly or indirectly, to support the financial institution's activities, particularly critical activities.

Service Provider Concentration (Financial sector) – The extent to which financial institutions rely on a service provider, directly or indirectly, to support financial institutions' activities, particularly critical activities.

---

[86] https://www.cisa.gov/sites/default/files/2023-06/principles_approaches_for_security-by-design-default_508c.pdf
[87] https://aws.amazon.com/lambda/serverless-architectures-learn-more/#:~:text=A%20serverless%20architecture%20is%20a,management%20is%20done%20by%20AWS.
[88] https://www.fsb.org/wp-content/uploads/P091219-2.pdf
[89] Adapted from https://learn.microsoft.com/en-us/azure/aks/servicemesh-about
[90] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-292.pdf
[91] https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-response-soar
[92] https://cloudsecurityalliance.org/cloud-security-glossary#A

Service Provider Concentration Risk (Financial Institution) - The potential for disruption or degradation at a service provider(s) to threaten the ability of a financial institution to continue performing the financial institution's activities, particularly critical activities, or cause the financial institution to suffer significant adverse effects.

Service Provider Concentration Risk (Financial Sector) - The potential for disruption or degradation at a service provider(s) to threaten the ability of financial institutions to continue performing their activities, particularly critical activities, or cause the financial institutions to suffer significant adverse effects, with the potential for systemic impact to the financial sector.

Shared Responsibility - The division of responsibilities between the CSP and the cloud customer for the design, configuration, and operation of the cloud environment, including those concerning security obligations. [93]

Software as a Service (SaaS) - A cloud service model that provides the capability to the cloud customer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The cloud customer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.[94]

Software Bill of Materials (SBOM) - A formal record containing the details and supply chain relationships of various components used in building software. Software developers and vendors often create products by assembling existing open source and commercial software components. The SBOM lists these components for a given product.[95]

Standard Image - The approved set of server configurations, applications, and systems, which can be used to deploy servers consistently and rebuild them more easily and quickly, when necessary.[96]

Supply Chain - Linked set of resources and processes between and among multiple levels of entities, each of which is an acquirer, that begins with the sourcing of products and services and extends through their life cycle.[97]

Supply Chain Risk - The potential for harm or compromise that arises as a result of security risks from suppliers, their supply chains, and their products or services. Supply chain risks include exposures, threats, and vulnerabilities associated with the products and services traversing the supply chain as well as the exposures, threats, and vulnerabilities to the supply chain.[98]

---

[93] https://aws.amazon.com/compliance/shared-responsibility-model/
[94] https://csrc.nist.gov/glossary
[95] https://csrc.nist.gov/glossary
[96] https://ithandbook.ffiec.gov/glossary/
[97] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf
[98] https://csrc.nist.gov/glossary/term/supply_chain_risk

Tenant - One or more cloud service customers sharing access to a set of physical and virtual resources.[99]

Vendor Lock-in - A situation whereby an entity is unable to easily change its service-provider either due to the terms of a contract, a lack of feasible alternative providers, or technical features.[100]

Virtualization – A software process that enables the hardware resources of a single computer, processors, memory, storage and more to be divided into multiple virtual computers, called virtual machines. It also allows multiple guest virtual machines to run on a host operating system. Guest virtual machines can run on one or more levels above the host hardware, depending on the type of virtualization.[101,102]

Virtual Machine - A digital version of a physical computer. Virtual machine software can run programs and operating systems, store data, connect to networks, and do other computing functions, and requires maintenance such as updates and system monitoring.[103]

[99] https://www.iso.org/obp/ui#iso:std:iso-iec:22123:-1:ed-2:v1:en
[100] https://www.fsb.org/wp-content/uploads/P091219-2.pdf
[101] Adapted from https://www.ibm.com/topics/virtualization?mhsrc=ibmsearch_a&mhq=virtualization
[102] Adapted from https://docs.aws.amazon.com/glossary/latest/reference/glos-chap.html#A
[103] https://cloud.google.com/learn/what-is-a-virtual-machine

Cloud Computing Terms and Definitions Primary Sources

The Financial Services Sector's Adoption of Cloud Services - US Treasury

FFIEC Glossary

NIST SP 500-292 Cloud Computing Reference Architecture

NIST SP 800-204 Security Strategies for Microservices-based Application Systems

NIST SP 800-190 Application Container Security Guide

NIST Glossary

CISA - NICCS (National Initiative for Cybersecurity Careers and Studies)

CISA Cloud Security Technical Reference Architecture

CISA Principles Approaches for Security by Design Default

Cloud Information Center - Cloud Basics

FSB Third-party Dependencies in Cloud Services: Considerations on Financial Stability Implications

FSB Enhancing Third-Part Risk Management and Oversight: A toolkit for financial institutions and financial authorities

Cloud Security Alliance Cloud Security Glossary

ISO/IEC :22123-1:2023(en)

Microsoft Azure Glossary

Google Terms

Amazon Glossary

IBM Cloud Glossary

ISACA Glossary

Gartner IT Glossary

ITIL Glossary