FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/IEC
FDIS
5140**

ISO/IEC JTC **1**/SC **38**

Secretariat: **ANSI**

Voting begins on:
2023-10-25

Voting terminates on:
2023-12-20

Information technology — Cloud computing — Concepts for multi-cloud and the use of multiple cloud services

Reference number
ISO/IEC FDIS 5140:2023(E)

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

Published in Switzerland

Contents

Page

Foreword

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

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

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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

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

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 38, *Cloud computing and distributed platforms*.

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

Introduction

Cloud service customers (CSCs) create cloud solutions that satisfy their requirements and benefit from the use of cloud computing. In creating these cloud solutions, CSCs sometimes use cloud services from multiple cloud service providers (CSPs). The use of multiple CSPs gives rise to cloud deployment models (CDM) such as hybrid cloud, multi-cloud and hybrid multi-cloud. Similarly, the CSPs themselves sometimes utilize cloud services from other CSPs resulting in CDMs such as inter-cloud and federated cloud.

The use of cloud services from multiple CSPs, either through CSC cloud solutions or by CSPs utilizing cloud services from other CSPs, can potentially enhance availability, resilience, fault-tolerance, latency, flexibility, business continuity, cost optimization, the ability to operate in multiple geographies or jurisdictions, and the ability to meet compliance requirements. On the other hand, use of multiple cloud services in general and multiple cloud services from multiple CSPs can result in increased complexity and other operational and administrative challenges. These challenges, which can manifest in various ways, are addressed in order to create a cloud solution. Examples of such challenges include the integrations and data transformations that would be necessary; additional burdens on management, logging, monitoring and error resolution; the reconciliation of the cloud service agreements and cloud SLAs from multiple CSPs; the complexity of total cost estimation; identity management and access control that works across multiple CSPs; and privacy.

This document provides an overview of, and foundational concepts for, cloud computing involving multiple cloud service providers (CSPs). This document establishes a common understanding of cloud solutions that use cloud services from multiple CSPs by building on the cloud computing concepts defined in the ISO/IEC 22123 series. It also provides characteristics, benefits and challenges relating to multi-cloud and other cloud deployment models involving multiple CSPs.

Information technology — Cloud computing — Concepts for multi-cloud and the use of multiple cloud services

1 Scope

This document specifies foundational concepts for multiple cloud services including multi-cloud, hybrid cloud, inter-cloud and federated cloud.

2 Normative references

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

ISO/IEC 22123-1, *Information technology — Cloud computing — Part 1: Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 22123-1 apply.

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

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

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

4 Symbols and abbreviated terms

API	application programming interface
CDM	cloud deployment model
CSA	cloud service agreement
CSC	cloud service customer
CSF	cloud service federation
CSN	cloud service partner
CSP	cloud service provider
CSU	cloud service user
IDaaS	identity as a service
PII	personally identifiable information
SLA	service level agreement
SO	service objective

5 Notational conventions

This document follows the same notational conventions and language used in the ISO/IEC 22123 series when it refers to parties, roles and sub-roles. The major parties of cloud computing are cloud service customer (CSC), cloud service partner (CSN), and cloud service provider (CSP). These parties are entities that play roles (and sub-roles). The major roles of cloud computing are cloud service customer role (CSC role), cloud service partner role (CSN role), and cloud service provider role (CSP role). These roles can be further organized into sub-roles. It is important to note that a party can play more than one role at any given point in time and may only engage in a specific subset of activities of that role. As an example, "CSC" refers to the cloud service customer party and "CSC role" refers to the cloud service customer role.

Within this document, the name of a sub-role has the prefix of "CSC:" for CSC sub-roles, "CSN:" for CSN sub-roles, or "CSP:" for CSP sub-role and then the sub-role name. Table 1 shows the prefix for each of the three cloud computing roles.

Table 1 — Cloud computing sub-roles

Role	Sub-role prefix	Example
CSC role	"CSC:"	CSC:cloud service user
CSN role	"CSN:"	CSN:cloud auditor
CSP role	"CSP:"	CSP:network provider

6 Cloud computing using multiple CSPs

6.1 General

It is sometimes challenging to find an appropriate complete cloud solution from a single CSP that fully meets the organization's requisite needs. A strategy that includes cloud services from multiple CSPs enables cloud solutions that go beyond the capabilities of any single CSP.

There are several cloud deployment models (CDMs)[1] that involve multiple CSPs. These include, but are not limited to:

— **multi-cloud** (see Clause 7)

— **federated cloud** (see Clause 8)

— **hybrid cloud** (see Clause 9)

— **hybrid multi-cloud** (see subclause 9.6)

— **inter-cloud** (see Clause 10).

There are three fundamental approaches for CDMs that involve multiple CSPs:

— The CSC controls and manages the cloud services that are being delivered by each of the CSPs including the orchestration of the cloud solution; one example is a multi-cloud.

— One CSP combines the cloud services from multiple CSPs with varying degrees of orchestration, control and management activities; one example of this is an inter-cloud in which the CSC interacts with only one CSP.

— Multiple CSPs form a partnership through out-of-band collaboration and share their resources via cloud services; one example of this is a federated cloud.

These approaches are not mutually exclusive and it is possible to combine them.

The presence of multiple CSPs, and consequently of multiple cloud services, creates additional challenges for governance, access control, sharing of resources, trust, security and privacy that should be addressed.

The implementation of a CDM that involves multiple CSPs should take into consideration the location of data centres, connectivity among them, data locality, management of instances, failure models, and error propagation. For example, appropriate cloud service agreements, cloud SLAs and interoperable single sign on are implemented by co-operating CSPs.

6.2 Interactions among parties

In a single CSP cloud solution, most interactions are between the CSC and the CSP. For the multiple CSP environment, the nature of the interactions depends on the CDMs being used for the cloud solution. The choice of CDM affects the responsibilities of each party within the cloud solution, the cloud SLAs between the parties, the cooperation required from the parties involved and the data path/flow among the parties.

Interactions among parties involved in cloud solutions consisting of multiple CSPs include:

— **Interactions between the CSC and the CSPs**: Interactions between the CSC and the multiple CSPs involved in the cloud solution depend on the CDM being used. For example, in the inter-cloud case, the CSC interacts only with a single primary CSP and it is that primary CSP's responsibility to use the cloud services of the secondary CSPs to provide cloud services that the CSC needs. This is unlike the multi-cloud case, where the CSPs involved are potentially unaware of each other and the CSC provides the necessary orchestration activities required to create the cloud solution.

— **Interactions among CSPs**: Each CSP offers cloud services that can be similar to or different from the cloud services offered by the other CSPs that are part of the cloud solution. The CSPs can be collaborating with each other, or they can be unaware of each other’s involvement in the CSC’s cloud solution. This can result in different CDMs being used in the cloud solution. For example, in the multi-cloud case, it is the CSC that is responsible for the orchestration and the data transformations/translations that are needed to create the cloud solution, with the CSPs not necessarily aware of each other. Whereas in the case of federated cloud, the multiple CSPs are aware of each other and cooperate with each other to share resources and data within a CSF domain.

Each of these interactions among the parties can be further classified as:

a) **Operational interaction**, which is used for delivering the services that are required.

b) **Management and administration interaction**, which are used to manage, administer the services, and support security and privacy capabilities.

7 Multi-cloud

7.1 General

In a multi-cloud CDM, the CSC is responsible for providing cloud service administrator and business manager functions for a defined set of cloud service users (CSUs) (i.e. domain of control over a set of end users and their activities). The operational interactions between the CSC and the CSP(s) are for the CSUs while the management and administration interactions support the administrator and manager activities.

Multi-cloud CDMs can be divided into two sub-types:

— **CSC-mediated multi-cloud**: Multi-clouds in which all interactions are between the CSC and the CSPs. See subclause 7.2.1.

— **CSP-connected multi-cloud**: Multi-clouds in which some or all interactions are between the CSPs' data centres but are initiated, controlled and managed by the CSC or code under CSC's control. See subclause 7.2.2.

In multi-cloud solutions, the CSC has a cloud service agreement (CSA), which includes a cloud SLA, with each of the CSPs separately. Each cloud SLA may be different in terms of capabilities being provided, the qualities of the services, the period and locations of service delivery, and the costs associated with the services.

7.2 Multi-cloud sub-types

7.2.1 CSC-mediated multi-cloud

In a CSC-mediated multi-cloud solution the CSC selects cloud services offered by two or more CSPs. Multi-cloud is the term used to describe the situation where one CSC uses public cloud services from two or more CSPs. This is shown in Figure 1, in which a CSC uses one cloud service from CSP1 and another cloud service from CSP2. The essence of multi-cloud, which differentiates it from other forms of interoperation of multiple cloud services, is that decision-making and control of the use of the multiple cloud services lies with the CSC. In a CSC-mediated multi-cloud solution, the CSPs involved are possibly but not necessarily aware of the multiple cloud services being used.

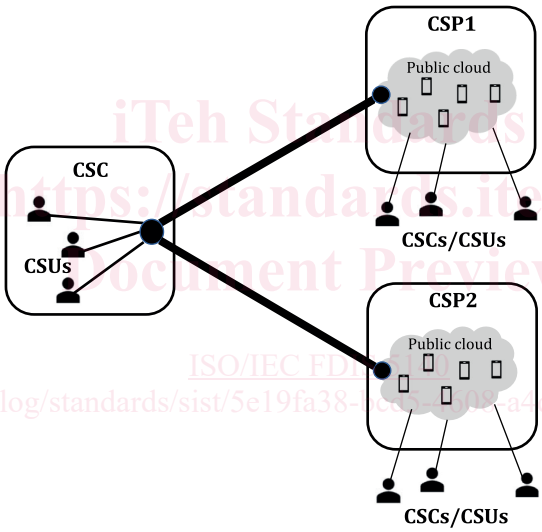

Figure 1 — Basic multi-cloud example

While the multiple cloud services can be used independently by the CSC, for the multi-cloud case the CSC creates a cloud solution by combining the cloud services offered by multiple CSPs. It is the CSC's responsibility to apply any necessary data translation, data transformations and integration functions.

One example is when the output of one cloud service is used to create input for a second cloud service, organized by the CSC, such that the two cloud services involved are unaware of each other's existence.

7.2.2 CSP-connected multi-cloud

The different cloud services can be used together more directly as shown in Figure 2. For example, a compute service from CSP1 can use a storage service from CSP2. In this case, the compute service uses the APIs of the storage service to store or read data from the storage service. It is the CSC that organizes the enablement of the API used in the code deployed in the cloud service at CSP1 or the configuration at CSP1 to use the storage service at CSP2.

In Figure 2, where the data is processed (CSP1) and stored (CSP2) by different CSPs, the CSC has a cloud SLA with CSP1 to address compute-related service objectives (SOs) and another SLA with CSP 2 to address storage related SOs such as data storage locations and controls. Additionally, in this example

the CSC requires that the compute service used at CSP1 has connectivity to access the storage service at CSP2.

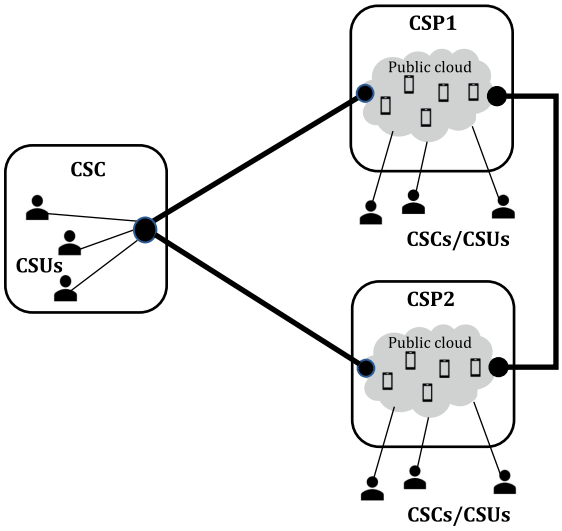

Figure 2 — Example of a multi-cloud with an inter-CSP connection

In the case of a web application, typically there is a user interface component that consists of the code that serves up the web pages, a business logic component that has the code to perform business transactions and a database component that holds the data used within the application.

Figure 3 shows that the user interface service (CSP1) uses the business logic service (CSP2), while the business logic service (CSP2) uses the database service (CSP3). The solution is organized by the CSC by configuring the relevant cloud services. In this case each component is implemented using a cloud service from a different CSP.

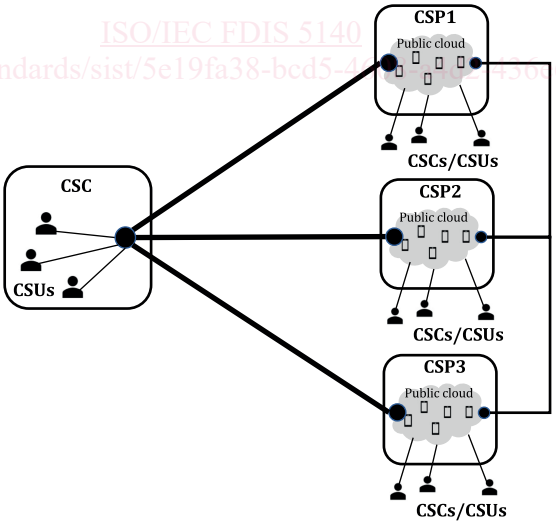

Figure 3 — Example of a more complex multi-cloud

In Figure 3, it can be the case that the use of the business logic service by the user interface service is arranged by the CSC through configuration of the code in the user interface service. The same pattern applies to the use of the database service by the business logic service.