International Standard

ISO/IEC 5140

First edition
2024-01

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

Technologies de l'information — Informatique en nuage — Concepts pour le multi-nuage et l'utilisation des services en nuages multiples

Reference number
ISO/IEC 5140:2024(en)

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 necessary integrations and data transformations; additional burdens on management such as 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 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.

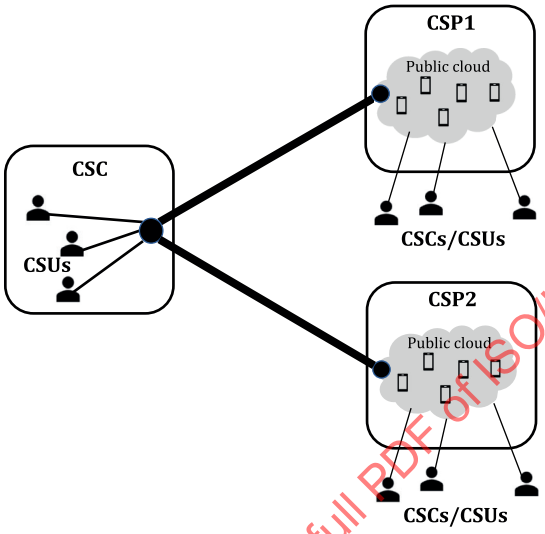

Figure 1 — Basic multi-cloud example

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.

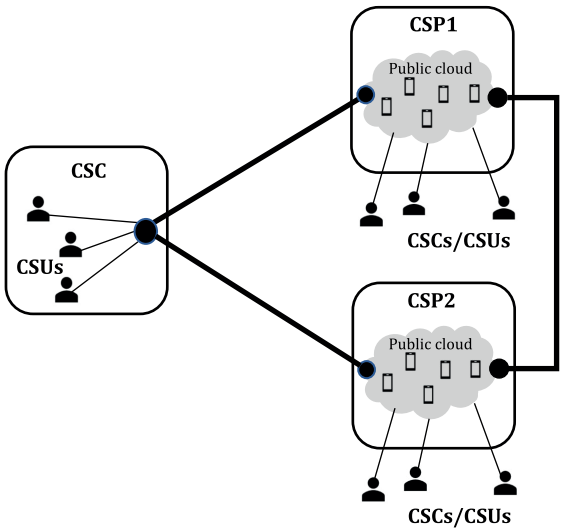

Figure 2 — Example of a multi-cloud with an inter-CSP connection

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.

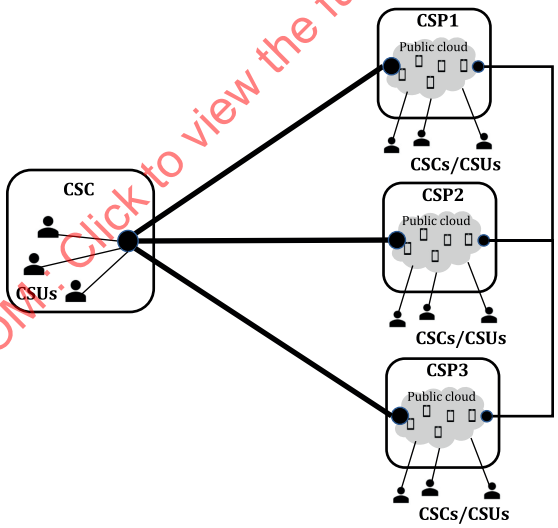

Figure 3 — Example of a more complex multi-cloud

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.

7.3 Characteristics

Since multi-cloud is a CSC-driven CDM, the participating CSPs are not necessarily aware of each other. The requirements of the CSC provide the reasons for choosing multi-cloud.

Multi-cloud can be used for the following cloud capabilities types for the reasons listed:

— **Application**: Some applications are only available from specific CSPs, potentially leading to a mix of CSPs. The CSC may require integration of cloud services offered by different CSPs.

— **Platform**: CSPs may specialize in the business or technical platforms that are required for specific applications.

— **Infrastructure**: Different CSPs can provide customized or specialized resources or offer infrastructure services in different cloud regions or availability zones.

In addition, a multi-cloud can be a mix of CSPs that offer different application, platform and infrastructure capabilities types.

At its most fundamental, multi-cloud is an extension of cloud computing to include public cloud services from more than one CSP. Multi-cloud inherits all the standard benefits of a public cloud. The key characteristics of multi-cloud are derived directly from those of cloud computing as described in the ISO/IEC 22123 series. These are:

— **Broad network access**: Network accessibility is a key characteristic for all cloud services in a multi-cloud environment. CSCs benefit from a wider selection of cloud access points. Broad accessibility can improve resilience and minimize single points of failure. Access to inter-CSP networks can also be required.

— **Measured service**: Services that are measured and pay-as-you-go permit multiple CSP cost optimization and workload distribution including across jurisdictions.

— **Multi-tenancy**: Extensions across CSP boundaries provide additional opportunities for the CSC to partition its CSUs into tenancies that use cloud services from different CSPs. For example, a CSC can choose to partition its CSUs into different tenancies based on which CSP services they access.

— **On-demand self-service**: Self-service operations and management automation become more critical when multiple CSPs are involved. Multi-cloud requires integrated multiple CSP operations and management.

— **Rapid elasticity and scalability**: Multi-cloud provides additional options for elasticity and scalability such as balancing workloads across multiple CSPs and global optimization of cost, performance, and functionality.

— **Resource pooling**: A CSP typically aggregates or pools resources in order to serve multi-tenant CSCs. In the case of multi-cloud, the CSC can use a service-based approach to optimize the use of the underlying resources offered by the cloud service of the multiple CSPs.

Additional characteristics that apply to multi-cloud include:

— **Cloud infrastructure independence**: Individual CSPs within a multi-cloud are physically and logically independent of each other and can provide different cloud services.

— **Cloud controls**: The CSC controls the multi-cloud and each CSP involved in the multi-cloud performs activities to its own cloud services according to the requested control by the CSC. These cloud controls can include activation, configuration, integration, orchestration and de-activation of each cloud service and its underlying resources.

7.4 Benefits

Multi-cloud provides a wide range of possibilities for cloud solutions that are not limited to a single CSP. Potential benefits of multi-cloud include:

— **Flexibility**: Multi-cloud facilitates the “mixing and matching” of CSPs and their cloud services. Multi-cloud configurations can provide enhanced resilience, wider distribution, extended functionality, stronger security, and possibly reduced overall cost. Service flexibility applies to application, platform, and infrastructure capabilities types.

EXAMPLE 1 Compute services are often chosen to minimize latency, to take advantage of network resources or to be close to storage. In the case of edge computing[2] that uses a multi-cloud solution, different CSPs can be selected for different geographical regions.

— **Availability**: A multi-cloud environment occurs when one CSP does not offer all the required cloud services. In some cases, a cloud service is only available from specific CSPs, either globally or in specific locations.

EXAMPLE 2 A CSC requires a specific weather service that is available from only one CSP. The service is not portable, so the CSC chooses that CSP's weather service. If the CSC's application itself is hosted by another CSP, then a multi-cloud solution would be required.

— **Best of breed**: Different CSPs offer "best of breed" solutions for the different cloud services needed by a CSC. By choosing each cloud service on its own merits, the CSC ends up using multiple CSPs.

EXAMPLE 3 A company acquires storage services from different CSPs based on price, storage requirements, affinity with other services, sharing requirements, or other criteria such as company policy.

— **Fault-tolerance**: A CSC can choose two or more CSPs for a given set of cloud services to enhance fault-tolerance in case the cloud services from one CSP become unavailable for some reason. This is an alternative to the use of regions and availability zones of a public cloud from one CSP.

EXAMPLE 4 Diversification of storage in the previous example is used to avoid a single point of failure. At least two storage services would be selected, with the choice made for each CSU or by department or division.

— **Proximity and latency:** It can be the case that different CSPs have their cloud service resources in different geographic regions and that, for proximity and latency reasons, the CSC chooses two or more CSPs in order to meet the performance requirements of the CSUs.

EXAMPLE 5 The resources available from a CSP will vary by cloud region, and there will be differences in the specific cloud services that are available. If a CSC can select a CSP that is close to the CSC, then quality of service improvement is possible. Edge computing is an example where edge services may not be available everywhere from the same CSP.

— **Data residency**: Data residency requirements can dictate the use of more than one CSP.

EXAMPLE 6 Data residency issues may occur if a single CSP does not have coverage in all required areas or is not able to securely store data in all jurisdictions.

EXAMPLE 7 Data residency issues may require data to be stored in a particular jurisdiction, location or with specific CSPs. In data backup cases there may be a requirement for data to not be stored in a particular location.

— **Regulatory requirements**: Some aspects of cloud computing are subject to local regulatory controls, which potentially are not met by all CSPs. The ability to select a CSP that meets local requirements is important for designs that include data residency, data disclosure, criminal laws, cross-border data flow and possibly tax regimes.

EXAMPLE 8 Certain financial data and banking information cannot be stored outside the country of origin. Since a CSP's cloud services vary in their degree of compliance with applicable regulations, the CSC benefits by choosing the CSP to maximize adherence to local regulations and conditions.

— **Cost**: Multi-cloud provides opportunities to manage costs by choosing the most effective overall solution and through negotiating more favourable discounts. This, however, should be balanced against increased complexity and an increased need for automation and control.

EXAMPLE 9 Multiple CSPs can offer similar services using different pricing models and conditions, possibly dependent on volume, time, location or other discounting criteria. A CSC with a multi-cloud solution can more easily move data or workloads to take advantage of lower costs.

7.5 Considerations

The use of multi-cloud results in several challenges that should be addressed.

— **Complexity**: Settings, defaults, security controls and functionality can vary across CSPs. Interacting with different CSPs with different processes and interfaces can make it harder for a CSC to manage its use of cloud services. The CSC can rationalize the interfaces and processes to create a unified multi-CSP dashboard or user interface. There can be additional considerations for multi-cloud management, such as identity brokering, cloud service discovery, routing, network and connectivity.

— **Latency**: While multi-cloud can potentially provide the benefit of reducing overall application latency, it can increase latency between the cloud services provided by different CSPs that frequently interact. This can be significant if the communicating cloud services are distant. Multi-cloud management should account for such latency variances.

— **Performance**: Different CSPs can have different cloud SLAs and therefore the associated service level guarantees can be different. Any use of multi-cloud should account for these differences.

— **Cost estimation and optimisation**: Different CSPs can have different cost structures and billing practices. A multi-cloud deployment that is trying to constrain and optimise costs should take this into account.

— **Logging and monitoring**: An application that uses cloud services from multiple CSPs should collect telemetry from each cloud service, analyse it and provide operational insights. Given the potential differences in the content, format and associated metrics, as well as how and when the data is available from the different CSPs, multi-cloud management should account for all these differences. This can require providing unified capabilities for monitoring, logging, tracing and analytics for cloud services across different CSPs.

— **Cloud service level agreements**: When an application makes use of multiple CSPs, in which each CSP provides a unique cloud service that is not replicated elsewhere, the overall availability of the application depends on the availability of each cloud service provided by the independent CSPs. For example, the configuration shown in Figure 3 requires that the three services provided by CSP1, CSP2 and CSP3 be available for the overall application to be available. This results in application availability that is lower than the availability of each individual service. The CSC should take reliability into consideration when evaluating cloud SLAs.

— **Privacy of data**: Data privacy in a multi-cloud solution is quite complex. It can be challenging to comply across all CSP cloud services with respect to data protection requirements while identifying, monitoring, processing, sharing and moving sensitive data. The implementation of policies, privacy and security controls across CSPs can be important in meeting regulations, laws and governance rules.

— **Assessment and compliance**: CSCs should understand the regulatory requirements, laws, and governance for developing a compliance strategy. They should consider the implications of using multi-cloud solutions that involve multiple CSPs in potentially different jurisdictions. CSPs can have different approaches to addressing compliance and regulation. Considerations include, though are not limited to, data residency, data use, criminal laws, cross-border data flow and tax regimes. CSCs should involve many stakeholders to formulate and design a strategy that satisfies many pertinent components such as legal, technological and administrative.

— **Workforce technical skills**: Incorporating public cloud services provided by different CSPs would require the CSCs to have workforce with sufficient skills to operate, maintain and handle the diverse cloud services and technologies involved.

7.6 Multi-cloud management

Multi-cloud management includes managing the use and operation of multiple public cloud services from two or more CSPs. Since the CSPs or the cloud services that they offer are not necessarily aware of each other, the primary responsibility for management of a multi-cloud solution lies with the CSC.

Different CSPs provide different capabilities, interfaces, data centre locations, provisioning mechanisms, connectivity, security and access protocols. Ideally multi-cloud management would provide a consistent way to manage the provisioning of cloud services across multiple cloud services and CSPs including:

— access

— security

— connectivity

— logging and monitoring of resources and services

While a multi-cloud manager need not be a separate operational entity, Figure 4 shows the capabilities needed for such a multi-cloud manager.

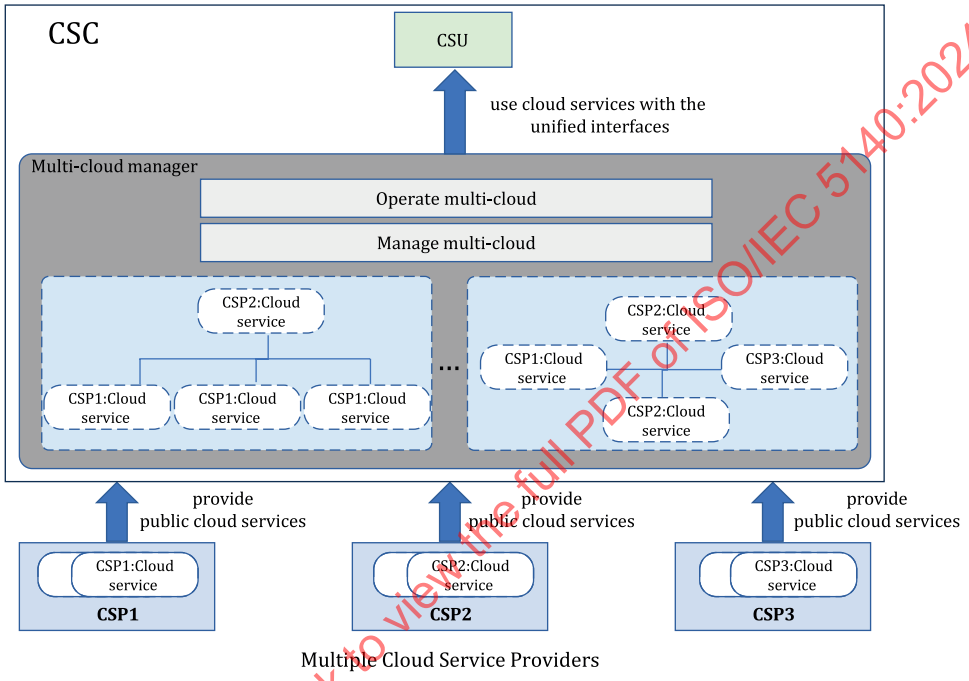

Figure 4 — Basic functions of multi-cloud management

The multi-cloud manager, implemented by the CSC, is responsible for identifying the cloud services offered by public clouds that meet CSC's requirements and orchestrating any additional needs such as load balancing, connectivity, high availability, monitoring and logging. The multi-cloud manager provides the means for accessing, managing and operating the cloud services. The operational capability of a multi-cloud manager can include the ability to manage the lifecycle of a multi-cloud solution. Annex A lists a few use cases that illustrate the complexities of, and the need for, multi-cloud management.

8 Federated cloud

8.1 General

A federated cloud is a CDM in which cloud services are provided by two or more members of a cloud service federation (CSF). A CSF is a collaboration among CSPs that is designed to support the sharing of resources. To be part of a CSF means agreeing to the policies, rules, standards, mechanisms and federated cloud SLAs (which are part of CSAs) by which the resources will be shared among the CSF members. In this case, federated cloud SLAs represent cloud SLAs that are established internally in the federation between member CSPs.

A cloud SLA is an agreement between a CSC and a CSP (see ISO/IEC 19086-1). A federated cloud offers cloud services to the members of the CSF. In that context, the federated cloud SLA is an agreement between the

member of the CSF that uses the cloud service (and therefore has the CSC role) and the federated cloud (which has the CSP role).

The existence of a federated cloud SLA does not preclude additional agreements between specific CSF members.

Note that CSF members may offer cloud services to parties that are not CSF members. Such cloud services are outside the scope of this document and can require a separate cloud SLA.

There is a great variety of ways that resources can be arranged within a CSF (see subclause 8.7). Some of the more common elements that dictate how the resources are arranged include: the focus on the purpose of the CSF; how identity management is managed; and how the resources are shared, discovered, managed, and paid for by the users of the cloud service. It is possible to establish a CSF to share a specific type of resource such as a database or other information.

An example of a CSF formed to share a specific type of information would be several organizations, acting as CSPs, coming together to share medical data such as genomic sequencing. In this case, the focus of the CSF is to provide access to the scientific information rather than moving the data around. The federated cloud supports local computations on these very large data sets. Since this is often speculative research it is also likely that, in this example, the CSF would have limited data costs–there would be a one fee access policy or even reduced costs for small data searches. It is likely that they would also set up policies and access controls that would emphasise fast data searches on very large data sets (similar to many of the problems faced by big data).

Another example of a CSF is an industry supply chain or ecosystem, where suppliers and their customers form a trust framework to share relevant data using cloud services. In this case, the metadata of relevant data may be broadly shared, whereas the data itself may be limited to a peer-to-peer sharing.

Federated clouds designed around a specific purpose would likely deploy the cloud resources in a way that optimizes its purpose—resulting in design decisions prioritizing transaction performance, CSF member independence, resilience, regulatory compliance or other parameters as necessary.

One issue that is common to all CSFs and federated clouds is how identity management will be handled. A federated cloud governed by a CSF can have any number of different identification schemes. Often viewed as a topological map to show relationships between CSF members, a federated cloud can be (see subclause 8.7 for more details):

— Centralized, with a single entity providing all identity management;

— Hierarchical, where responsibilities are delegated from the parent to the child in the hierarchy;

— Peer-to-peer, where each member of the CSF performs their own identity management (also called decentralized);

— Some other distributed topology or a combination of multiple topologies.[4]

Another issue that impacts a federated cloud is what resources are available from the CSF members and how those resources are paid for by the end user. Theoretically, a CSF can have access to all of the data and resources available to its members. However, it is unlikely that would be used except in limited situations. In most cases, a CSF member would have a set of resources that they would want to make available to other CSF members and an expectation of how they would be reimbursed for those resources (usually being paid for the resources, but options such as reciprocity are also possible). A CSF member should understand how the CSF functions to know what resources are available and at what cost. A CSF has a discovery system to allow each CSF member to advertise availability and what requirements, such as pricing or usage requirements, are associated with those resources.

8.2 Benefits

Federated clouds offer similar benefits to multi-clouds in that they offer a wide range of possibilities for cloud solutions by not being limited to cloud services offered by a single CSP. However, since they are bound

by a set of cloud computing management policies and activities that the parties agree to use, CSFs can offer some other benefits.

— **Trusted environment**: A CSF provides a trusted environment for collaboration with clear membership criteria and policies. The CSF is responsible for delivering and enforcing the essential trust and policy requirements for activities within the CSF.

— **Dynamic membership**: One of the main advantages of a CSF is that it is an organization that allows for a changing membership of CSPs. A CSF can provide mechanisms for adding and removing members. New cloud services can be added to a CSF simply by adding a new member offering those cloud services. By having a common set of management policies and activities, a federation streamlines and simplifies the process of adding new members.

— **Federated cloud SLA support**: One of the main challenges associated with multiple cloud interaction is the development of suitable cloud SLAs. For example, each party in the multiple cloud interaction needs to establish a cloud SLA with each other. This can be a time-consuming process as each cloud SLA is usually developed independently. In addition, adding new CSPs potentially requires an update to or renegotiation of SLAs with existing CSPs. A CSF, on the other hand, can establish federated cloud SLA that will be used to govern the interactions between the CSF members. A federated cloud SLA both facilitates the addition of new CSF members and sets a common level of guarantees between CSF members.

— **Identity management**: In order to operate within a CSF requires the ability to perform identity management, which includes mechanisms to provide authentication, authorization, and accountability. A CSF can establish its own internal mechanism of providing those services to its members.

— **Shared Benefits**: As a CSF grows each individual member gains shared benefits. More cloud services offered by the CSF members will lead to more use of those cloud services in the CSF.

8.3 Considerations

While Federated clouds offer many benefits they also come with additional challenges and concerns.

— **Security and privacy**: CSF identity management can be compromised by a single participant with lax controls. The more participants in a CSF the greater the number of potential points of vulnerability.

— **Losing resources**: Loss of a CSF member that has critical capabilities or change in its policies (subject to the agreements of the CSF) can leave the remaining members without needed resources. A CSP that depends on resources from other CSF members can be left with no suitable replacements.

— **Inadequate discovery services**: A CSF shares knowledge about services that are available to CSF members. CSF members can exist in a variety of different administrative, legal, or geographical domains. A CSF discovery service should maintain not just information about services and costs, but all the details that can factor into a CSC being able to use a given service.

8.4 Cloud service federation

8.4.1 Characteristics

Given the wide applicability and sheer variety of possible federated clouds, it is critical to understand the key characteristics of CSFs. The following are the key characteristics:

— A CSF is a secure and trusted sharing collaboration that is not necessarily owned by any one entity or organization.

— CSF members collaborate for common goals and have identity credentials that can be used within the CSF.

— Entities and organizations can participate in a CSF by choosing to share some of their resources and metadata and making them discoverable and accessible to other CSF members.

— Participating members agree upon the common goals and governance of their CSF, based on common activities, attributes and policies.

— A CSF establishes a common cloud SLA or a uniform way to handle federated cloud SLAs between the CSF members to facilitate the joining of new members. Without such a mechanism, each potential new member negotiates cloud SLAs with each existing member prior to joining.

8.4.2 CSF membership

A CSF is a set of CSPs that are its members, for some definition of membership. Each CSF may define its membership based on a set of specifications. Some CSFs may allow users to self-identify and join with essentially no identity proofing or new member vetting. Other CSFs may have stricter requirements in this regard. Some CSFs may have definite expectations or conditions of membership that each member is expected to observe. Joining a CSF can also require specific legal agreements.

8.4.3 Shared resource metadata and discovery

While the types of resources to be shared can be open-ended, each CSF has certain resource types that are commonly shared to meet the goals of the CSF. These data and services should be clearly identified and described with some well-known metadata. Therefore, this represents a potential semantic interoperability requirement that will typically be addressed by standardized schemas and ontologies.

After a CSF is instantiated, various member resources should be made available to and accessible by the other members. There should be a mechanism in which members can discover available resources and services; for example through the use of a resource catalogue and discovery service. The details of how these catalogue and discovery services and their semantics are implemented can be CSF-specific. Likewise, the resource discovery policies associated with the catalogued resources can be CSF-specific, and based on CSF-specific metadata attributes and roles or attributes associated with any member that is searching the catalogue.

In some circumstances, the CSF members may jointly agree to define the discovery policy for the different types of available sources so that the goals of the CSF can be met. In other situations, however, the resource owner may wish to define the discovery policies for their own resources. In this case, CSPs can participate in a CSF by selectively making some of their resources discoverable and accessible by other CSF members. These policies are based on the resource metadata, roles, and attributes defined within the CSF. If a CSF only involves a small, fixed set of services that each member offers to any other member, then the resource catalogue and discovery process become very simple. In the more general case, however, there will be a definite need for resource metadata and service discovery policies.

The availability of a metadata store to list and describe the CSF resources supports the CSF members by sharing vetted information about said resources and services. Cryptographic signing of this metadata prevents its unauthorized modification.

Although the purpose of a CSF is to collaborate and share resources, the resource owners retain ultimate control over their own resources. Subject to the agreements of the CSF, a resource owner may unilaterally change their discovery and access policies. However, such unilateral policy changes can adversely affect other CSF members as well as the cloud service they are offering to the CSCs.

8.4.4 CSF governance

Participating members can jointly agree upon the common goals and governance of their CSF. That joint governance is expressed by the policies governing the roles and responsibilities of membership, resource discovery, and resource access.

There should also be a process to grant or revoke CSF membership. Assuming that members are not allowed to simply self-identify and join, then there should be a mechanism which allows granting and revoking memberships, and some entity, a CSF manager, that has the authorization to do so. This authorization can also be granted to specific CSF members. They would have the responsibility to enforce new member identity proofing or vetting policies, if any, such that an authorized and authenticated user can access a set of resources. If the CSF has any conditions that require membership revocation, then the CSF manager has

the responsibility to execute the revocation. The CSF manager may also have the responsibility to monitor, detect and verify when such conditions have occurred.

A CSF will also have a set of roles or attributes that are filled by its members. These roles and attributes define the responsibilities that different members have, or what actions they can take and use to make various policy decisions governing the operation of the CSF. The meaning of these roles and attributes should be well known to all members. Likewise, there should be a process to grant or revoke member roles or attributes. Assuming that not all CSF members are "equal" and cannot access all shared resources equally, then there should be some method of distinguishing among what different members can do. Depending on the CSF topology, assigning different roles or attributes to members would be carried out by one or more entities that has the authorization to grant and revoke member roles or attributes.

8.5 CSF domains

8.5.1 General

Members of a CSF can be in different or more than one domain and yet be tied together in a CSF. Two common domains that impact CSF members are administrative domains and regulatory domains.

8.5.2 Administrative domains

An administrative domain is a construct that represents a logical sub-grouping that can exist within a federated cloud. An administrative domain consists of two or more CSPs, identity management and administration for that domain.

Administrative domains typically operate as independent, autonomous environments with a federated cloud. The domain administrators will issue identity credentials, deploy services, and define the policies for who can access what. For example, the IT department at a large corporation will issue credentials to employees that enable them – based on company policies – to use email accounts and to access shared internal websites, databases, collaboration tools, etc.

These independent, autonomous environments are de facto identity silos outside of which a CSF member's credentials have no useful meaning. There is no easy, convenient way to securely manage the sharing of specific information and resources among such silos. An organization can establish a website that is accessible by the general public to make information available. However, to control access, general users are given accounts at that CSF member. That CSF member then determines which resources that user can access. Requiring users to have different accounts at each CSF member is simply not scalable or manageable. Even if users have different accounts at each CSF member, there is no coherent, consistent way for the CSF members to manage which resources the users can access for a common purpose or project. CSF enables the bridging of these identity silos whereby the participants can jointly define, agree upon, and enforce resource discovery and access policies.

8.5.3 Regulatory domains

Administrative domains exist within some regulatory environment. All CSCs and CSPs exist within the jurisdiction of some set of governmental entities and observe all relevant regulations defined by those entities. There can be multiple governmental entities at the national, state, and local levels. The users and service providers observe the union of the regulations defined therein. The CSF governance body determines the baseline compliance requirements and defines the strategies for identity and access to data and services in their regulatory environment. This is done through the identity and authorization credentials that are associated with users, and the access policies that are defined for any given resource. In addition, considerations for different personally identifiable information (PII) handling policies across disparate regulatory environments should include specific privacy requirements.

8.6 CSF management sub-roles

8.6.1 General

Specific CSF sub-roles can optionally be established to manage and run the CSF itself. Since the members of the CSF are CSPs, these sub-roles are CSP sub-roles. Depending on the topology (see subclause 8.7), one or more members of a CSF can play these sub-roles. Examples of these sub-roles include but are not limited to:

— CSP:CSFOperator

— CSP:CSFManager

— CSP:CSFAuditor

— CSP:CSFBroker

8.6.2 CSF operator

A CSF operator provides the functions needed to enable, manage, maintain and oversee the overall operation of one or more CSF managers. The CSF operator is superior to the CSF manager and CSF auditor. For CSF members that participate in multiple separate and distinct CSFs, a CSF operator will coordinate the activities of the CSF managers and provide administrative support and maintenance by collecting, processing, and resharing individual CSF metadata while following the common policies and legal frameworks shared among CSFs. However, not all CSFs have a need for a CSF operator. In simpler instances, the CSF manager may be as simple as a server that does the management of a CSF.

8.6.3 CSF manager

The CSF manager provides the essential management functionality over the lifespan of a CSF. A CSF manager can support multiple CSFs that span multiple administrative domains.

The CSF manager occupies a place that is unique to the CSF model. The CSF manager establishes and operates a CSF across multiple CSF members. It is required to perform a number of critical management functions over the lifespan of a CSF instance.

The CSF manager is not necessarily a single, separate party. Federated cloud environments can include one or more CSF managers, each of which is operated by a CSF operator. A single CSF operator can oversee multiple CSF managers in either centralized or decentralized configurations. As the scale and magnitude of the CSF increases, the presence and activities of the CSF operator become more pronounced.

8.6.4 CSF auditor

In the broadest sense, a CSF auditor can be an independent third party that can assess compliance for any type of policy associated with a CSF. Responsibilities of a CSF auditor are similar to those of a cloud auditor, but its scope is across the entire CSF. This list is a cursory overview of possible CSF-specific auditing requirements:

— **Usage and performance audit**: Some CSFs may want to audit for usage and performance, perhaps in support of evaluating service level agreements associated with the CSF.

— **Membership audit**: CSF membership may come with a set of expectations as a condition of membership. A CSF auditor can assess whether members are complying.

— **Security, privacy and trust audit**: This encompasses all security and privacy issues but with the added concern that a CSF relies on multiple trust relationships. Security, privacy and trust can be based on auditing for acceptable configuration, privacy, confidentiality, minimal release of identity attributes, etc. In the same way that members may have requirements, CSF managers may have similar requirements that can be audited.

— **Regulatory audit**: Since CSFs may span different regulatory environments, a CSF auditor may be required to assess whether joint and local regulations are being observed. The CSF policy management

and enforcement relies on a review of these documents and how they affect the adherence to both membership, and security and trust.

8.6.5 CSF broker

CSF members require the functionality of a cataloguing system to enable discovery and sharing of resources in a federated cloud. The discovery service categorizes cloud services, resources and data based on specific properties.

Beyond discovery and cataloguing, a CSF broker enables the following functionality:

— Service intermediation which allows CSF members to provide value-added service where an existing cloud service from a CSF member can be enhanced.

— Service aggregation which combines and integrates multiple cloud services, possibly from different CSF members, into one or more new cloud services.

— Service arbitrage which is similar to the service aggregation but with a flexible dynamic choice. In practice this function can give preference, for similar characteristics, CSF participants that follow the members specific needs such as to save money, or to be more local, or other member specific criteria.

The CSF broker allows members to decide between services and resources provided by other CSF members. CSF members benefit from the service arbitrage functionality. In order for the CSF broker's functionality to be useful to CSF members, a CSF broker should continuously update its metadata, relationships between CSF members, general CSF information, as well as the available cloud services and resources in its resource catalogue.

8.7 CSF topologies

The functionality of a CSF manager is often depicted as being provided by a single entity. However, it is a conceptual entity that provides the essential management functionality and as such can exist in multiple entities within a federated cloud. A good way to look at possible CSF topologies is to understand how the CSF manager functionality is deployed. Topologies have differing effects on functionality, governance, and discovery.

A centralized topology has a single CSF manager as shown in Figure 5. All participating CSF members trust the CSF manager and its CSF operator to manage the CSF and can include access to information about the participants within the CSF and can authorize new members to join.

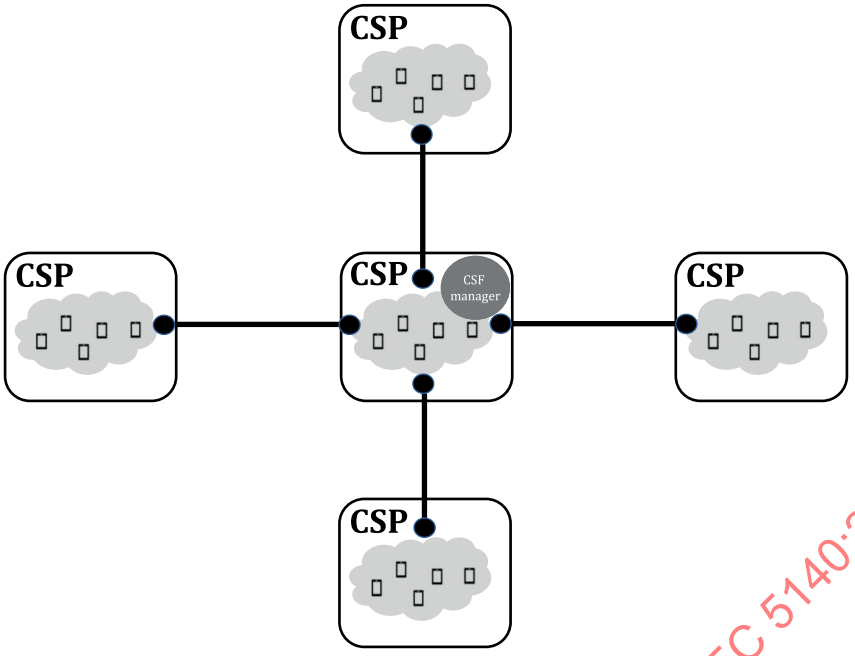

Figure 5 — Centralized topology example

Figure 6 illustrates a peer-to-peer topology, where all CSF managers are peers to one another. In this model there is no central coordinator and there is implicit trust between all members.

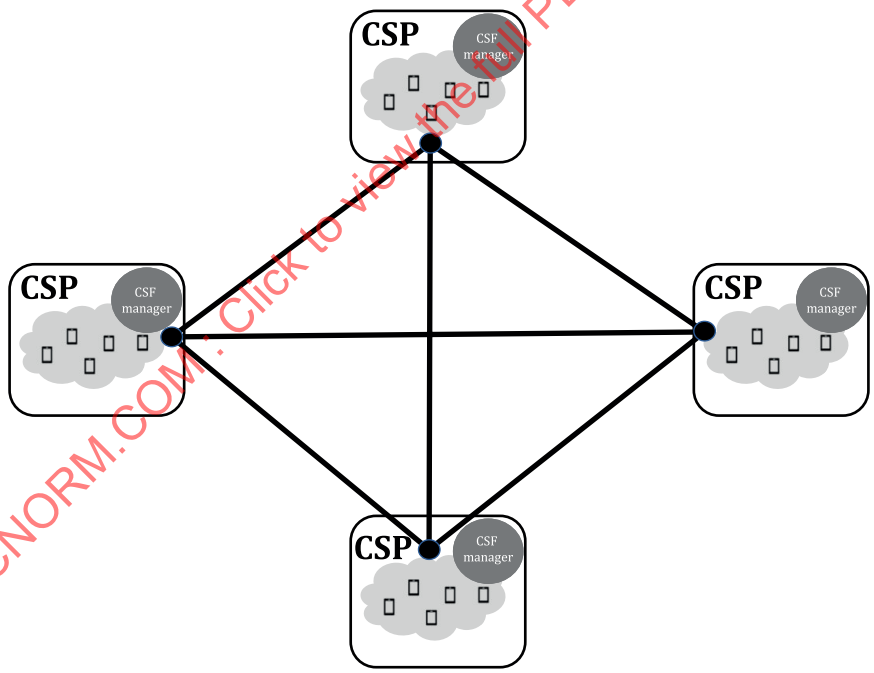

Figure 6 — Peer-to-peer topology example

Figure 7 illustrates a hierarchical topology, where CSF managers exist in a parent-child relationship. The parent CSF manager defines the governance for the child CSF manager.

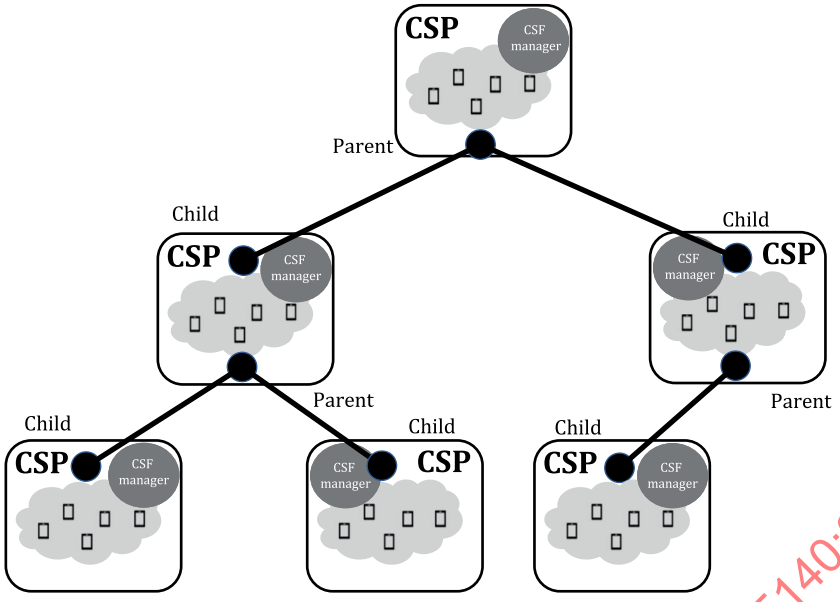

Figure 7 — Hierarchical topology example

The topologies listed above are not exhaustive and other distributed topologies are also possible including combination of multiple topologies.

It is possible for a CSP to be a member of more than one CSF. Figure 8 illustrates an example of a CSP (CSP3) that is a member two CSFs (CSF1 and CSF2).

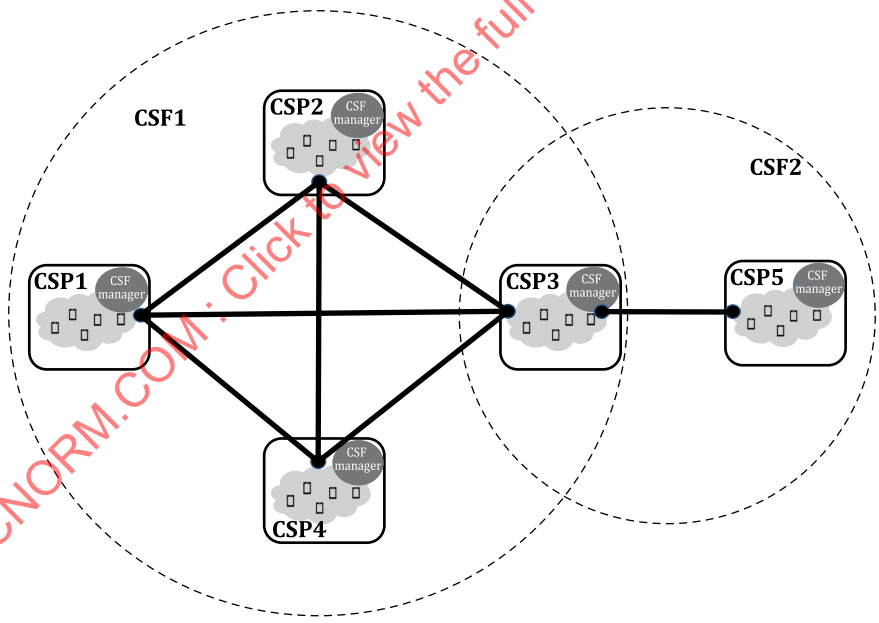

Figure 8 — Overlapping CSFs example

9 Hybrid cloud

9.1 General

A hybrid cloud is a CDM that uses both a public cloud and a private cloud, as illustrated in Figure 9. The public and private clouds involved remain unique but are bound together by appropriate technology that enables interoperability, data portability and application portability.

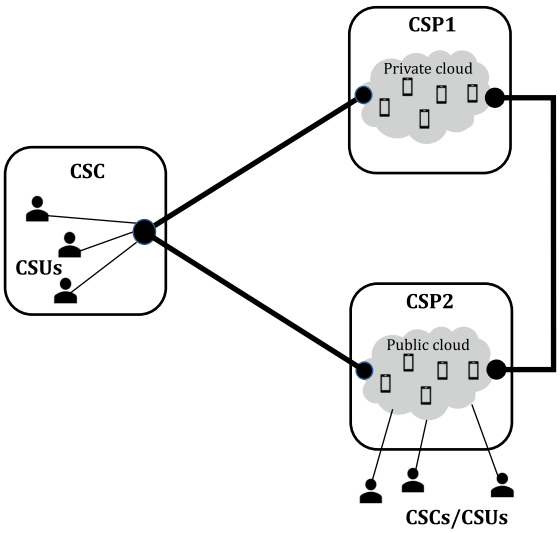

Figure 9 — Example of a hybrid cloud CDM

Hybrid cloud represent configurations in which direct interaction between the private and the public cloud may be needed and is enabled through appropriate technologies.

The three hybrid cloud configurations are:

— the public and private clouds are managed and operated by the same CSP,

— the public and private clouds are managed and operated by different CSPs, and

— the private cloud is managed and operated by the CSC and the public cloud is managed and operated by a CSP.

In all these three cases, the resources in the private cloud are controlled by the CSC. The CSC can directly access the private cloud, the public cloud or both.

9.2 Characteristics

Hybrid cloud is an extension of cloud computing to include a composition of a private cloud and a public cloud. Hybrid cloud inherits all the basic benefits of a public cloud in much the same way that multi-cloud does.

Hybrid cloud is a CSC-driven deployment model. If multiple CSPs are involved in the hybrid cloud, in some cases they should be aware of each other's involvement in a cloud solution. This may be required in order to enable the appropriate technologies that allow interactions that are necessary for the cloud solution. The reasons for choosing hybrid cloud are derived primarily from the CSC's requirements which would include the need for cross-CSP coordination of the interactions.

Hybrid cloud is similar to multi-cloud in that it can also be used for the application, platform and infrastructure cloud capabilities types for the same reasons as multi-cloud (see subclause 7.3).

Additional characteristics that apply to a hybrid cloud include:

— **Cloud independence**: The private and public parts of the hybrid cloud are physically and logically independent and may provide different cloud services. They also support the appropriate technologies for direct interaction.

— **Cloud controls**: The CSC controls the hybrid cloud but can delegate specific control activities to a CSP. Cloud controls include activation, configuration, integration, orchestration and de-activation of each cloud service and its underlying resources including the appropriate technologies for direct interaction.

The main differences between a hybrid cloud and a multi-cloud are:

— the use of a private cloud to provide some of the required capabilities; and

— the binding together of the private and public parts of the hybrid cloud by appropriate technology to enable interoperability, data portability and application portability.

9.3 Benefits

Hybrid cloud provides benefits similar to those provided by multi-cloud in general (see subclause 7.4). An important benefit is distribution of the cloud services geographically and possibly across different providers.

EXAMPLE 1

The private cloud in a hybrid cloud CDM stores and processes data that is tightly controlled and cannot be processed in a public cloud for regulatory, privacy, security or business reasons. The public cloud in the hybrid cloud CDM stores and process data that is publicly available, such as public social network data and can scale quickly for less cost. The CSC combines the data and processing powers of the private and public cloud to provide the cloud solution that manages cost, security, privacy, business and regulatory requirements.

EXAMPLE 2

The hybrid cloud provides "burst" capabilities for offloading computing or storage during peak times. In this use case the private cloud is normally used but has limited resources. The public cloud can provide additional resources when workloads surpass the capabilities of the private cloud.

EXAMPLE 3

The hybrid cloud provides automated, real-time backup for data that is stored in the private cloud. It is not necessary for the CSC to initiate or control the interactions between the private and public clouds once they have been set up.

9.4 Considerations

The general challenges of cloud solutions involving multiple parties are identified in subclause 7.5.

Hybrid cloud challenges are reduced when both the public and private clouds are managed and operated by a single CSP. For this case the CSC works with a single CSP and the cloud SLAs (which are part of CSAs) can be consolidated.

Complexity increases when the CSC manages and operates the private cloud, but in this case the CSC has control over what technologies are to be used for the interactions.

The hybrid cloud is most challenging when the private cloud is managed and operated by a third party that is not the same as the public cloud CSP. A cooperation agreement between the third party and the public cloud CSP would help to minimize the challenges in this configuration.

9.5 Hybrid cloud management

Hybrid cloud management is similar to multi-cloud management (see subclause 7.6 and Figure 4). When the private and public clouds are managed and operated by the same CSP, management functions can be consolidated.

Cloud management includes various controls including the activation, configuration, integration, orchestration and de-activation of each cloud service and its underlying resources. For a hybrid cloud this includes controls for the appropriate technologies that are needed for direct interactions.

The private cloud component in a hybrid cloud may be managed and operated by the CSC itself or by a third party and may be located on premises or off premises.

NOTE The CSC cannot be the operator of the public cloud that is used in the hybrid cloud.

In the case where there are two different cloud SLAs corresponding to the private and the public clouds, it is the combination of these two SLAs that is considered for satisfying the CSC's needs.