Singapore Accreditation Council

ACCREDITATION SCHEME FOR
MANAGEMENT SYSTEMS CERTIFICATION BODIES

CT 14
SAC CRITERIA FOR CERTIFICATION BODIES (MULTI-TIERED CLOUD COMPUTING SECURITY)

CT 14, 21 Dec 2020
The SAC Accreditation Programme is managed by Enterprise Singapore

1 Introduction

1.1 This document specifies the supplementary SAC criteria for Certification Bodies (CBs) certifying Multi-Tiered Cloud Computing Security (MTCS) management system.

1.2 This document is to be used with ISO/IEC 17021-1 and applicable IAF Mandatory Documents. Please refer to ISO/IEC *17788 Information technology — Cloud computing — Overview and vocabulary* for terms & definitions.

2 Certification Criteria

2.1 CBs shall certify organisations to (1) SS 584:2015 *Specification for Multi-tiered Cloud Computing Security* or (2) SS 584:2020 *Specification for Multi-tiered Cloud Computing Security.*

2.2 All SS 584:2015 certifications shall expire or by withdrawn by 31 Oct 2022.

3 Criteria for MTCS Auditors

3.1 A certification body shall appoint qualified auditors to conduct MTCS audits.

3.2 Auditors shall meet the criteria as defined in **Annex A (Normative)** of this document.

4 Duration of MTCS Audits

4.1 Where applicable, references shall be made to IAF Mandatory Document 5 (IAF MD 5).

4.2 In determining the audit duration, a CB shall determine the number of personnel doing work under the organisation's control for all shifts.

4.3 For initial audit, the starting point for an average audit duration (Stage 1 + Stage 2) shall be as indicated in **Table 4-1**.

Table 4-1: Relationship between Number of Personnel and Audit Duration

Number of Personnel doing Work under the Organisation's Control	Initial Audit Duration (Stage 1 + Stage 2)
1-10	5 auditor days
11-25	6 auditor days
26-45	7 auditor days
46-65	8 auditor days
66-85	9 auditor days
86-175	10 auditor days

Number of Personnel doing Work under the Organisation’s Control	Initial Audit Duration (Stage 1 + Stage 2)
176-275	11 auditor days
276-425	12 auditor days
426-625	13 auditor days
626-875	14 auditor days
876-1,175	15 auditor days
1,176-1,550	16 auditor days
1,551-2,025	17 auditor days
2,026-3,450	18 auditor days
3,451-4,350	19 auditor days
4,351-5,450	20 auditor days
5,451-6,800	21 auditor days
6,801-10,700	22 auditor days
>10,700	Follow progression above

a. For requirements for stage 1 and stage 2 audits, CBs shall refer to clause 9.3 of ISO/IEC 17021-1

b. The numbers of personnel in **Table 4-1** should be seen as a continuum rather than a stepped change.

c. The CB’s procedure may provide for audit duration for number of personnel doing work under the organisation’s control for all shifts exceeding 10,700. Such audit duration should follow the progression in **Table 4-1** in a consistent fashion.

d. Based on the impact level, additional auditor day shall be added. See clause 4.4.

4.4 Impact Level (as defined in table 4 of SS 584)

Table 4-2: Relationship between Impact Level and Additional Auditor Day

Impact Level	Additional Auditor Day (minimum)
Level 1- Low impact	0 auditor day added
Level 2- Moderate impact	1 auditor day added
Level 3- High impact	2 auditor days added

Table 4-2 is only applicable to

a. IaaS and PaaS (Infrastructure as a Service); or
b. SaaS (Software as a Service) with IaaS together

c. For certification of SaaS running on MTCS certified infrastructure, the audit man-days may be reduced up to 30%. The reduction is due to SaaS certification being done on an accredited MTCS certified infrastructure.

4.5 Multi-sites Audit

The size of the sample shall follow IAF Mandatory Document (MD) 1 on Audit and Certification of a Management System Operated by a Multi-Site Organisation.

4.6 Other factors to considered for determination of audit duration

a. No. of platforms or complexity of the cloud environment
b. No. of data centres
c. Risk level (low, medium, high)

4.7 Organisations with accredited ISO/IEC 27001 Certification

If an existing organization has already been certified to ISO/IEC 27001, CB may reduce the minimum number of auditor days as specified in **Table 4-1** by up to 50% provided the following conditions are met:

a. Certification scope of ISO/IEC 27001 is similar to the certification scope of SS 584

b. Computed auditor days after the reduction for initial audit is at least 5 auditor days

4.8 CB shall calculate the audit duration. In all cases where adjustments are made to the audit duration provided in **Table 4-1**, sufficient evidence and records shall be maintained to justify the variation.

4.9 In order to ensure effective audits being performed and to ensure reliable and comparable results, the audit duration provide in **Table 4-1** shall not be reduced by more than 30%. Appropriate reasons for the deviation shall be established and documented.

4.10 Surveillance audit duration shall be 1/3 of initial audit duration.

4.11 Recertification audit duration shall be 2/3 of initial audit duration.

4.12 If after the calculation the result is a decimal number, the number of auditor days should be adjusted to the nearest half day (e.g. 1.3 auditor days becomes 1.5 auditor days, 1.2 auditor days becomes 1 auditor day).

5 Scope Statement

5.1 The scope statement shall at least include the following:

a. Level of MTCS to be certified

i. MTCS Level 1: Non-business critical data or systems; or

ii. MTCS Level 2: Business critical data or systems; or
iii. MTCS Level 3: Specific requirements and more stringent security requirements

b. Name of service provider (legal entity)
c. Business address (office/operation address)
d. Name of services being certified, if the Cloud Service Provider (CSP) is offering different services or products
e. Service model or role of CSP. E.g. Infrastructure provider, application programming interface (API) or platform provider etc.
f. For MTCS level 2 and 3 certification - the data storage locations must be listed in appendix for information.
g. Where applicable, Compensatory Controls (CC) declared applicable/not applicable
h. Where applicable, extension of scope (See clause 5.3)

5.2 For example,

Level 2 of Multi-tier Cloud Security System (MTCS) of Company A located at <address> supporting the provision of ABC <service name> services using IaaS <service type> model

Compensatory Controls: XXXX (Version 1.0 dated XXX)

ABC’s services comprise of:
a) Compute Services <At location One>
b) Storage Services <At location One and location Two>

5.3 Extension of Scope

MTCS certification scope may be optionally extended to cover risks associated with recent technological changes or advancements such as Cloud Native environment as captured in TR 82 Guidelines for Cloud Native Security. In the event that the CSP chooses to extend scope to include TR 82, the ‘should’ mentioned in the TR 82 Cloud Native shall become a mandatory requirement (i.e ‘should’ will become ‘shall’). Where mandatory requirements are excluded, it shall be properly documented as per clause 6 of this document. The extension of scope shall be mentioned as per clause 5.1.h of this document.

Cloud native technologies empower organisations to build and run scalable applications in modern, dynamic environments such as public, private, and hybrid clouds. Containers, service meshes, microservices, immutable infrastructure, and declarative APIs exemplify this approach. Specifically, TR Cloud Native defines three common characteristics of Cloud Native architecture to scope its recommendations, for example:

a. Use of Container technologies
b. Use of Microservices-based technologies
c. Use of DevOps pipeline

6 Applicability and Compensating Controls

6.1 Generally, all the main clauses and critical clauses (e.g. clause 18.6 physical security) shall be applicable.

6.2 Depending on risk assessment and type of service, some exclusions may be allowed in SS 584:2020 *Specification for Multi-tiered Cloud Computing Security*. **Annex B (Informative)** of this document provides examples of exclusions of controls and design/use of compensating controls. The level of security or validity of MTCS certification shall not be compromised with the control exclusions and design/use of compensatory controls.

7 Additional Guidance

7.1 The Scope and ICT Supply Chain consideration is available in **Annex C (Informative)**.

7.2 Guidance for Certification of Different Types of Cloud Services is available in **Annex D (Informative)**

Annex A (Normative)

Criteria for MTCS Auditors

The summary of the criteria for MTCS Auditors is shown in **Table A-1**.

Table A-1: Summary of Criteria for MTCS Auditors

<table>
<tr><th>Criteria</th><th>MTCS Auditor</th><th>MTCS Lead Auditor</th></tr>
<tr><td>Ethics & attributes</td><td colspan="2">1. Demonstrates personal attributes for effective and efficient performance of audits
and
2. Generally, auditors should follow ISO/IEC 27007:2020 Information security, cybersecurity and privacy protection – Guidelines for information security management systems auditing</td></tr>
<tr><td>Qualifications and Experience</td><td colspan="2">1. <u>Degree in Information Technology/Computing</u>
At least 4 years full time working experience which includes minimum of 3 years full time professional work experience in Information Systems auditing, control or security work experience
or
2. <u>Diploma in Information Technology/Computing</u>
At least 5 years full time working experience which includes minimum of 3 years full time professional work experience in Information Systems auditing, control or security work experience</td></tr>
</table>

<table>
<tr><th>Criteria</th><th>MTCS Auditor</th><th>MTCS Lead Auditor</th></tr>
<tr><td>Auditor Training</td><td colspan="2">1. Successfully completed and passed
a. Certified Information Systems Auditor (CISA; or
b. Recognized Auditor / Lead Auditor course for Information Security management systems
and
2. Auditors with less than 2 years of experience working in cloud industry providing cloud service shall attend course on cloud knowledge with the following content:
a. Fundamental of Cloud computing:
i. Definition of cloud computing
ii. Components of cloud infrastructure
iii. Cloud computing model and operation
b. Cloud Computing Security
i. Infrastructure security for cloud computing
ii. Assessment of the infrastructure security for cloud computing
iii. Security basics of different cloud service models
iv. Security of Cloud computing deployment models
v. Data protection and security for cloud computing
vi. Security of cloud applications and users
vii. Knowledge in virtualization and technology
c. Manage cloud computing security and risk
i. Risk and governance
ii. Legal and compliance
iii. Audit
iv. Portability and interoperability
v. Incident response
In addition to the above, auditors (regardless of years of experience) auditing cloud native shall attend course on cloud knowledge with the following content:
a. Cloud Computing Security
i. Security of common technologies and techniques (such as container, micro-services and DevOps pipeline)</td></tr>
</table>

Criteria	MTCS Auditor	MTCS Lead Auditor
Audit Experience	Performed a minimum of 4 Information Security Management System (ISMS) audits as a qualified[1] ISMS auditor within a 2-year period with a minimum of 10 auditor days on site. The 2-year period shall be within immediate past 5 years.	Performed a minimum of 7 Information Security Management System (ISMS) audits as a qualified[2] ISMS auditor within a 2-year period with a. A minimum of 10 auditor days on site; and b. At least 3 of these audits shall be in the capacity as the lead auditor The 2-year period shall be within immediate past 5 years.
Maintenance of qualification (once every 3 years)	Performed a minimum of 5 MTCS[2] or ISMS audits at the end of an immediate past 3-year cycle	Performed a minimum of 5 MTCS[3] or ISMS audits at the end of an immediate past 3-year cycle with: a. At least 2 of these audits performed shall be in the capacity as the lead auditor

[1] Qualification of MTCS auditor can be done internally by the certification body to perform third-party MTCS audit

[2] MTCS or ISMS audits include initial, surveillance or recertification audits. 2nd party audits (supplier / vendor audits) performed based on SS 584 or ISO 27001 can be considered as audit experience stated in this document. All audits have to include the critical processes.

Annex B (Informative)

Examples of Control Exclusions and Use of Compensating Controls for SS 584:2020 Specification for Multi-tiered Cloud Computing Security

Examples of control exclusions and use of compensating controls is shown in **Table B-1**. This shall only be used when main control clauses can be excluded (Y) or partially excluded (P).

Table B-1: Examples of Control Exclusions and Use of Compensating Controls

Clause No.	Clause Description	Potential Exclusion for Cloud Model (Primarily focused on Level 1) [Yes(Y), No (N), Partial (P)]			Remarks on Potential Exclusion for Cloud Model	Compensatory Controls Description
		IaaS	PaaS	SaaS		
5	Cloud service provider disclosure	N	N	N	Not applicable	Not applicable
6	Information security management	N	N	N	Not applicable	Not applicable
7	Human resources	N	N	N	Not applicable	Not applicable
8	Risk assessment	N	N	N	Not applicable	Not applicable
9	Third party	N	N	N	Not applicable	Not applicable
10	Legal and compliance	N	N	N	Not applicable	Not applicable
11	Information security incident response plan and procedures	N	N	N	Not applicable	Not applicable
12	Data governance	N	N	N	Not applicable	Not applicable
13	Audit logging	N	N	N	Not applicable	CSP can monitor and review at least critical systems and system components (as defined by them) based on risk assessment
14	Secure configuration	N	N	P	SaaS CSP can	SaaS CSP can

Clause No.	Clause Description	Potential Exclusion for Cloud Model (Primarily focused on Level 1) [Yes(Y), No (N), Partial (P)]			Remarks on Potential Exclusion for Cloud Model	Compensatory Controls Description
		IaaS	PaaS	SaaS		
					a. Exclude clause 14.1 on Server and Network Device Configuration Standards b. Exclude clause 14.4 on Physical Port Protection if no network equipment like network switch is being used c. Exclude clause 14.7 on Unnecessary Service and Protocols if no network equipment like firewall is being used	a. Limit secure configuration only on their desktops and laptops OS if they do not have any servers or networks b. Replace clause 14.2 on Malicious Code Prevention (e.g Anti-virus (AV)) with other appropriate controls based on a risk perspective if they are running on non-windows environment.
15	Security testing and monitoring	N	N	N	Not applicable	Not applicable
16	System acquisitions and development	P	N	N	For IaaS CSP performing the provisioning of infrastructure services only, clause 16.4 on Source Code Security may not be applicable as they do not have software/system development and any software purchased are off-the-shelf software where source code is not provided. However, if the IaaS CSP also provides other SaaS services and is within the scope of certification, then this clause cannot be excluded	Not applicable
17	Encryption	N	N	N	Not applicable	Not applicable
18	Physical and environmental	N	N	P	Not applicable	SaaS CSP can limit its physical and environment security to office security

Clause No.	Clause Description	Potential Exclusion for Cloud Model (Primarily focused on Level 1) [Yes(Y), No (N), Partial (P)]			Remarks on Potential Exclusion for Cloud Model	Compensatory Controls Description
		IaaS	PaaS	SaaS		
						(e.g. access control to the office and CCTV). Equipment like gas Suppression system is not required but minimally, fire extinguishers should be available.
19	Operations	N	N	N	Not applicable	Not applicable
20	Change management	N	N	N	Not applicable	Not applicable
21	Business continuity planning (BCP) and disaster recovery (DR)	N	N	N	Not applicable	Not applicable
22	Cloud services administration	N	N	N	Not applicable	Not applicable
23	Cloud user access	N	N	N	Not applicable	IaaS CSP can exclude clause 23.9 on Self-service Creation and Management of User Accounts but it must come with an alternative control to manage its users
24	Tenancy and customer isolation	N	P	P	Not applicable	IaaS CSP can replace Storage Area Network (SAN) solution with other backup solutions

Annex C (Informative)

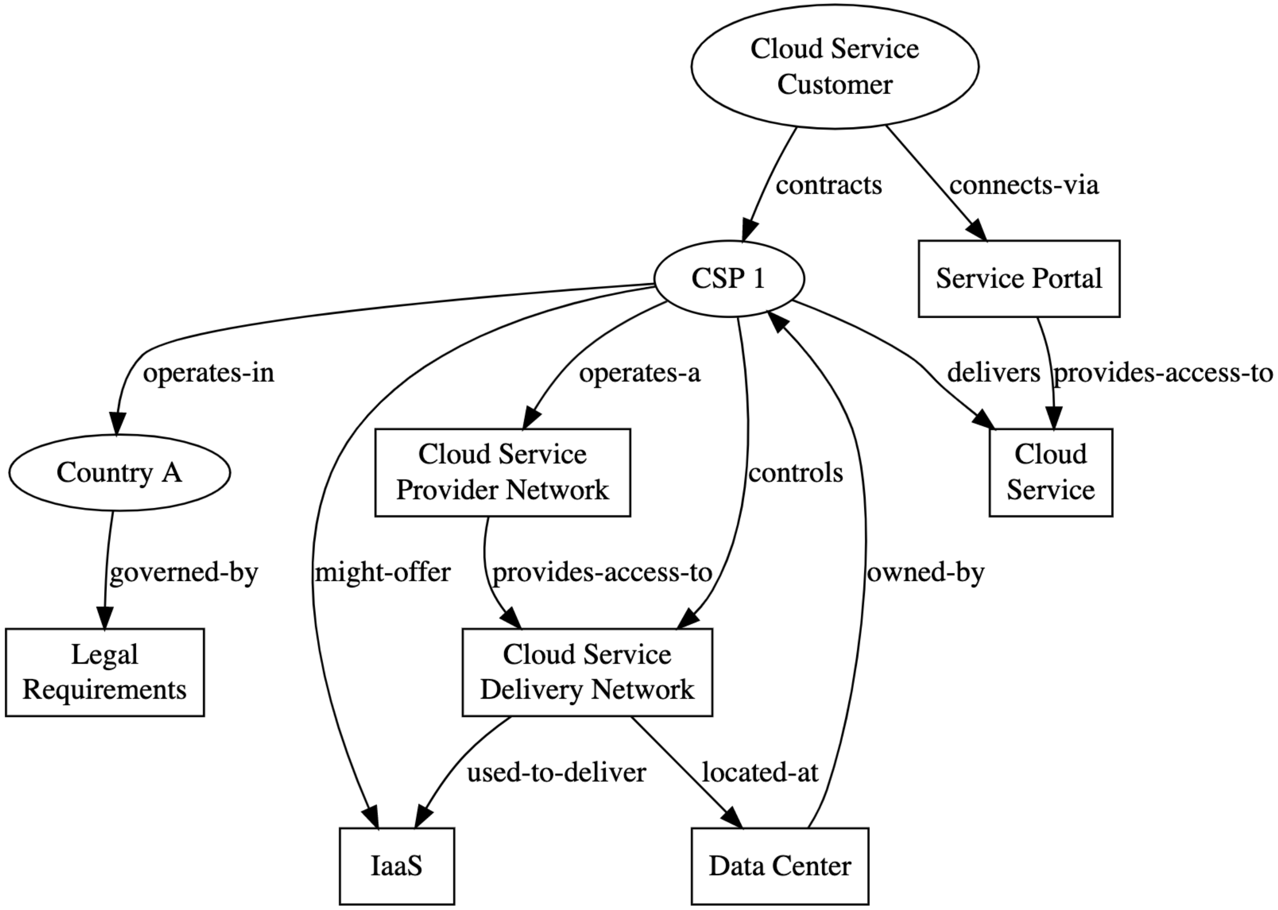
Scope and ICT Supply Chain Consideration - Four patterns to consider in scoping

1. Simple case

a. CSP Office located at one location, owns a DC in containing the infrastructure the same country and offers Cloud Services only in that country.
b. The Cloud service does not incorporate any service from another CSP and offers only IaaS
c. Customer service provided from its own servicer center
d. The cloud self provisioning portal is developed by itself
e. The cloud service network is bought out-of-the-shelf

The figure below shows relations of concepts, entities and interfaces to be considered in scope definition:

Figure C-1: Simple Case

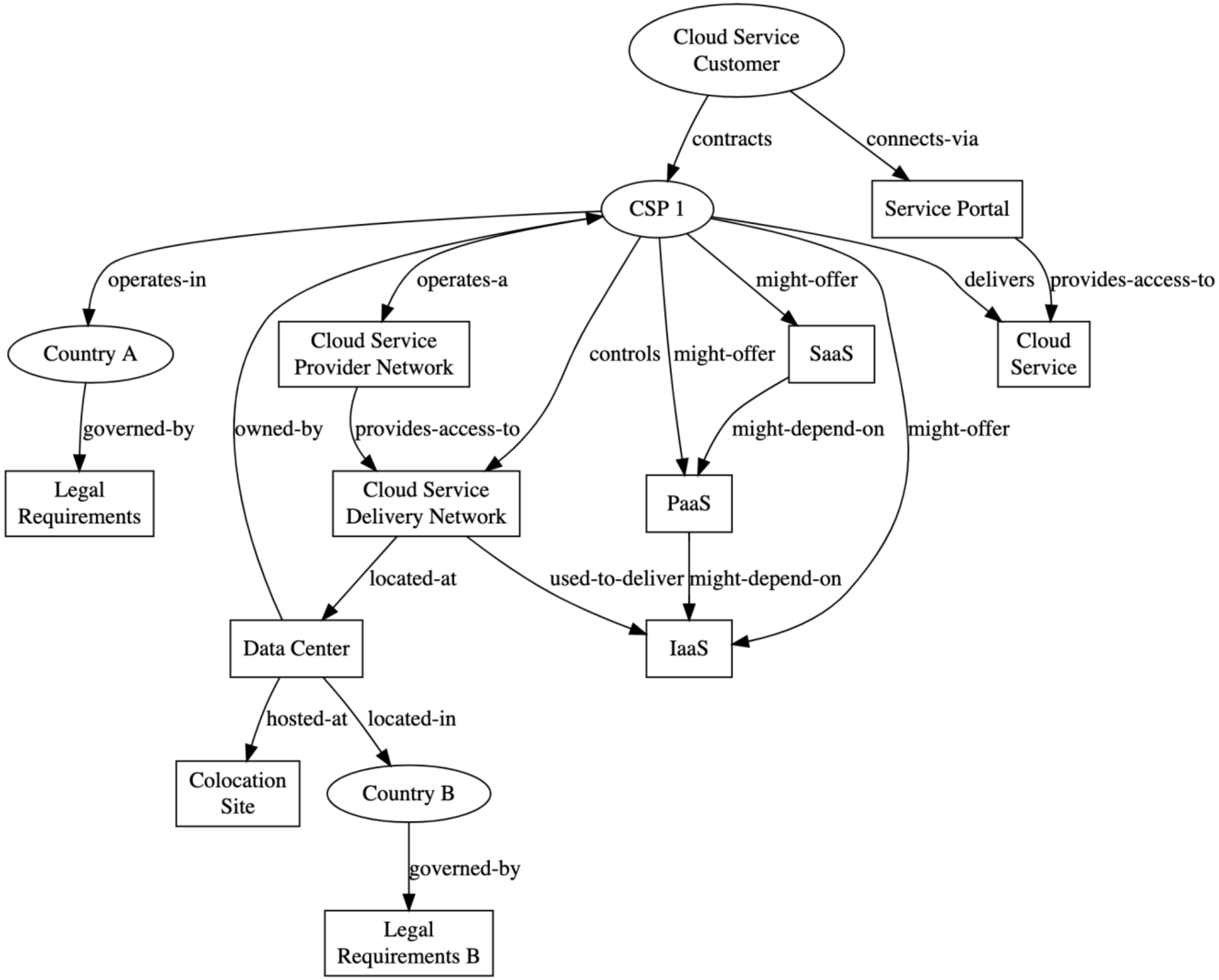


2. Common case

a. The CSP has several cloud capabilities and service categories
b. It has limited ownership over cloud technology or build on openstack
c. Uses a colocation site and relies on utilities and services provided by the colocation provider
d. It operates in several countries under several legislations
e. The service portal is developed by a third party
f. Incorporates other’s cloud service solutions

The figure below shows relations of concepts, entities and interfaces to be considered in scope definition:

Figure C-2: Common Case

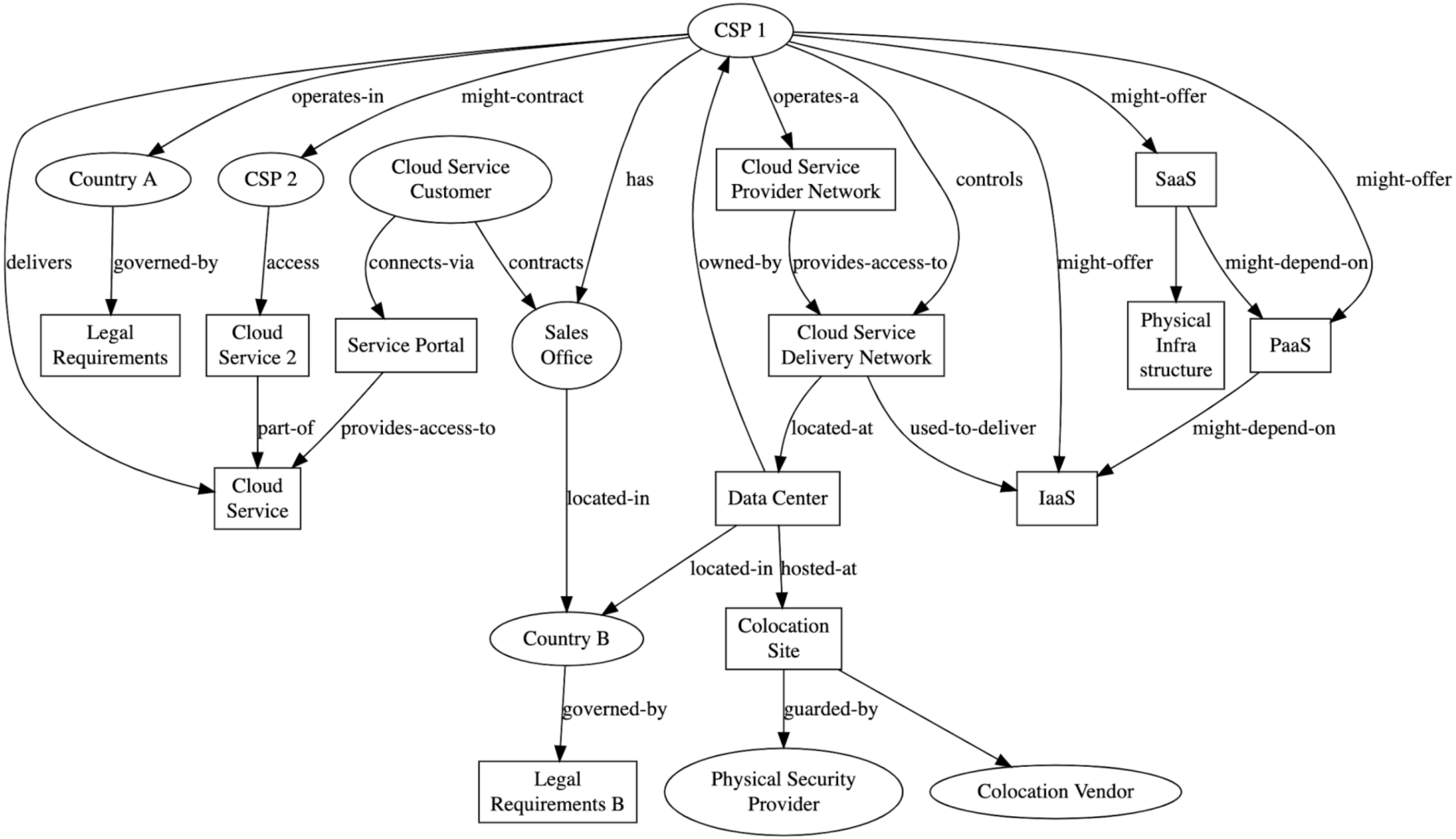


3. International CSP owning the technology

a. HQ in a country and cloud customers are from other country
b. The CSP has a sales office in a foreign country and concludes contracts under legal requirements of its country.
c. DC in a colocation site owned by another entity
d. Service offered regional
e. Incorporates other’s cloud service solutions

The figure below shows relations of concepts, entities and interfaces to be considered in scope definition:

Figure C-3: International CSP Owning the Technology



4. Telcom case

a. The CSP has limited or no cloud technology expertise and limited control over the development of the cloud delivery network components and its operation of a cloud management network depends on a technology provider.
b. The CSP brand the cloud service under its own brand but does not have governance over the cloud technology
c. Represented by a sales office acting as CSP in a legal sense

Annex D (Informative)

Guidance on Certification of Different Types of Cloud Services

1. How does MTCS certify SaaS?

    a. MTCS certification is about certifying cloud services offered by CSPs, not on a product or the CSPs.

    b. To certify SaaS under MTCS, besides the application/SaaS, the underlying infrastructure, network, platform, storage & data segregation (infrastructure & platform security), cloud operations and services administration needs to be audited/assessed end-to-end as per requirements.

    c. MTCS certification of a SaaS owned by an Independent Software Vendor (ISV) but hosted and offered at a cloud provider X cannot claim the same certification of the SaaS when hosted and offered at another cloud provider Y operating under a different infrastructure & platform environment. A separate independent MTCS audit/assessment for the provider Y underlying infrastructure is needed.

2. Should SaaS ISVs view the CSPs hosting them as their 3rd party (infrastructure) service providers and manage as such?

    a. Unless due diligence and thorough risk assessment have been performed, considering all clauses as defined by the standard for the 3rd party as per clause 9.1.2, the underlying infrastructure, network, platform, storage & data segregation, cloud operations and services administration, compliance of underlying infrastructure to MTCS standards cannot be assumed.

3. What are the most effective ways to have SaaS MTCS certified?

    a. SaaS ISVs could host its application/software on a MTCS certified infrastructure (IaaS) service to ensure the underlying infrastructure and network are already in compliance with MTCS standards.

    b. The certification of SaaS could then focus on its application/software integration and interfaces with the underlying certified infrastructure, network, platform, storage & data segregation, both technically and operationally, to achieve end-to-end security as per requirements

4. What are the levels that SaaS ISVs could be certified when hosted on a MTCS certified (IaaS) infrastructure service providers?

    a. If the underlying infrastructure (IaaS) service provider has been certified to MTCS level X, the SaaS hosted in this certified infrastructure can only be, at best, certified to same MTCS level X (or lower levels).