ETSI GS NFV-REL 005 V1.1.1 (2016-01)

GROUP SPECIFICATION

Network Functions Virtualisation (NFV); Accountability; Report on Quality Accountability Framework

Disclaimer

This document has been produced and approved by the Network Functions Virtualisation (NFV) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference

DGS/NFV-REL005

Keywords

NFV, quality

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Network Functions Virtualisation (NFV).

The present document deals with specific aspects of Service Quality Accountability in the context of Network Function Virtualisation.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

The NFV Quality Accountability Framework supports the quality management principles of customer focus ([i.7] principle **0.2.a**), mutually beneficial supplier relationships ([i.7] principle **0.2.h**) and factual approach to decision making ([i.7] principle **0.2.g**) to enable continual improvement ([i.7] principle **0.2.f**). Clearly defining roles, responsibilities and demarcations is a quality management best practice because it clarifies accountabilities which permit any quality impairments to be rapidly localized, root causes to be identified and appropriate corrective actions to be agreed to promptly restore service and drive continuous quality improvement. This informative document defines key roles including NFV cloud service customer, provider(s) of NFV management, orchestration and/or infrastructure services, and their VNF suppliers and Integrators. The document lays out the responsibilities for each role based on both extrapolating traditional responsibilities and considering responsibilities for each of the six essential characteristics of cloud computing. As objective and quantitative measurement is necessary to enable methodical quality assurance and management, the present document offers a quality measurement framework that connects standard metrics and measurements with roles, and an annex that offers sample service quality SLAs for a cloud service customer. A second annex offers use case scenarios illustrating how the quality accountability framework applies to several quality impairment scenarios.

This framework uses principles of ISO/IEC 17788 "Cloud computing -- Overview and vocabulary" [i.1] and ISO/IEC 17789 "Cloud Computing - Reference Architecture" [i.2] to the ETSI NFV architecture [i.12] to enable quality measurements consistent with both "TL 9000 Quality Management System Measurements Handbook" and "Network Functions Virtualisation (NFV); Service Quality Metrics" and SLA management consistent with TM Forum's "SLA Management Guidebook" and "Enabling End-to-End Cloud SLA Management."

1 Scope

The present document describes a quality accountability framework for NFV. This release focuses on service quality management of network services, VNFs, NFV infrastructure, management and orchestration elements.

The present document describes the following aspects of the Quality Accountability Framework:

1) **Roles**, covered in clause 4 *Roles in the NFV Ecosystem*.

2) **Responsibilities**, covered in clauses 5 *Responsibilities by Role* and 6 *Responsibilities for Key Cloud Characteristics*.

3) **Service quality measurements and demarcation points,** covered in clause 7 *Quality Measurement Framework*.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ISO/IEC 17788 (First edition) (2014-10-15): "Information technology -- Cloud computing -- Overview and vocabulary".

NOTE: Available at http://standards.iso.org/ittf/PubliclyAvailableStandards/c060544_ISO_IEC_17788_2014.zip.

[i.2] ISO/IEC 17789 (First edition) (2014-10-15): "Information Technology -- Cloud Computing -- Reference Architecture".

NOTE: http://standards.iso.org/ittf/PubliclyAvailableStandards/c060545_ISO_IEC_17789_2014.zip.

[i.3] TM Forum, TR 178 (V2.0.2) (October 2014): "Enabling End-to-End Cloud SLA Management", Framework Release 14.

NOTE: https://www.tmforum.org/resources/technical-report-best-practice/tr178-enabling-end-to-end-cloud-sla-management-v2-0-2/.

[i.4] TM Forum Guidebook GB917 (July 2012): "SLA Management Guidebook, Release 3.1".

NOTE: https://www.tmforum.org/resources/standard/gb917-sla-management-handbook-release-3-1/.

[i.5] QuestForum (Release 5.0, July 2012): "TL 9000 Measurements Handbook".

NOTE: Available at http://www.tl9000.org/handbooks/measurements_handbook.html.

[i.6] ETSI GS NFV-INF 010 (V1.1.1) (12-2014): "Network Functions Virtualisation (NFV); Service Quality Metrics".

[i.7] ISO 9000 (Third Edition) (September 2005): "Quality Management Systems - Fundamentals and Vocabulary".

[i.8] "Quality Measurement of Automated Lifecycle Management Actions", 1.0, August 18th, 2015, QuEST Forum.

NOTE: http://www.tl9000.org/resources/documents/QuEST_Forum_ALMA_Quality_Measurement_150819.pdf.

[i.9] ETSI GS NFV-MAN 001 (V1.1.1) (12-2014): "Network Functions Virtualisation (NFV); Management and Orchestration".

[i.10] ETSI GS NFV 003 (V1.2.1) (12-2014): "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[i.11] ETSI GS NFV-REL 004 (09-2015): "Network Functions Virtualisation (NFV); Active monitoring & failure detection report".

[i.12] ETSI GS NFV 002 (V1.2.1) (12-2014): "Network Functions Virtualisation (NFV); Architectural Framework".

[i.13] ISO 9001:2015: "Quality management systems -- Requirements".

[i.14] ISO 14001:2015: "Environmental management systems -- Requirements with guidance for use".

[i.15] ISO 27729:2012: "Information and documentation -- International standard name identifier (ISNI)".

[i.16] ISO/IEC 27001:2013: "Information technology -- Security techniques -- Information security management systems -- Requirements".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI GS NFV 003 [i.10] and the following apply:

audit: systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled

NOTE 1: Internal audits, sometimes called first-party audits, are conducted by, or on behalf of, the organization itself for management review and other internal purposes, and may form the basis for an organization's declaration of conformity. In many cases, particularly in smaller organizations, independence can be demonstrated by the freedom from responsibility for the activity being audited.

NOTE 2: External audits include those generally termed second- and third-party audits. Second-party audits are conducted by parties having an interest in the organization, such as customers, or by other persons on their behalf. Third-party audits are conducted by external, independent auditing organizations, such as those providing certification/registration of conformity to ISO 9001 [i.13] or ISO 14001 [i.14].

NOTE 3: This definition is from [i.7], clause 3.9.1.

cloud auditor: cloud service partner with the responsibility to conduct an audit of the provision and use of cloud services

NOTE: This definition is from [i.1], clause 3.2.3.

cloud computing: paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand

NOTE 1: Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

NOTE 2: This definition is from [i.1], clause 3.2.5.

cloud service: one or more capabilities offered via cloud computing invoked using a defined interface

NOTE: This definition is from [i.1], clause 3.2.8.

cloud service broker: cloud service partner that negotiates relationships between cloud service customers and cloud service providers

NOTE: This definition is from [i.1], clause 3.2.9.

cloud service customer: party which is in a business relationship for the purpose of using cloud service

NOTE1: A business relationship does not necessarily imply financial agreements.

NOTE 2: This definition is from [i.1], clause 3.2.11.

cloud service developer: sub-role of cloud service partner which is responsible for designing, developing, testing and maintaining the implementation of a cloud service

NOTE 1: This can involve composing the service implementation from existing service implementations.

NOTE 2: This definition is from [i.2], clause 8.4.1.1.

cloud service partner: party which is engaged in support of, or auxiliary to, activities of either the cloud service provider or the cloud service customer, or both

NOTE: This definition is from [i.1], clause 3.2.14.

cloud service product: cloud service, allied to the set of business terms under which the cloud service is offered

NOTE 1: Business terms can include pricing, rating and service levels.

NOTE 2: This definition is from [i.2], clause 3.2.2.

cloud service provider: party which makes cloud services available

NOTE: This definition is from [i.1], clause 3.2.15.

cloud service user: natural person, or entity acting on their behalf, associated with a cloud service customer that uses cloud services

NOTE 1: Examples of such entities include devices and applications.

NOTE 2: This definition is from [i.1], clause 3.2.17.

functional component: functional building block needed to engage in an activity, backed by an implementation

NOTE: This definition is from [i.2], clause 3.2.3.

party: natural person or legal person, whether or not incorporated, or a group of either

NOTE 1: This definition is from [i.1], clause 3.1.6 and was preceded by "*The following term is defined in ISO 27729*".

NOTE 2: The term *domain* used in [i.10] is not necessarily synonymous with party in that the perimeter of a particular domain is not required to be identical to the accountability perimeter of a particular party. For example, [i.9] states "*Administrative Domains can be mapped to different organizations and therefore can exist within a single service provider or distributed among several service providers*", which is consistent with "*Administrative Domains can be mapped to different organizations and therefore can exist within a single* ***party*** *or distributed among* ***several parties***."

private cloud: cloud deployment model where cloud services are used exclusively by a single cloud service customer and resources are controlled by that cloud service customer

NOTE: This definition is from [i.1], clause 3.2.32.

product category: recognized grouping of products for calculating TL 9000 measurements

NOTE: This definition is from the glossary of [i.5].

public cloud: cloud deployment model where cloud services are potentially available to any cloud service customer and resources are controlled by the cloud service provider

NOTE: This definition is from [i.1], clause 3.2.33.

quality: degree to which a set of inherent characteristics fulfils requirements

NOTE 1: The term "quality" can be used with adjectives such as poor, good or excellent.

NOTE 2: "Inherent", as opposed to "assigned", means existing in something, especially as a permanent characteristic.

NOTE 3: This definition is from [i.7], clause 3.1.1.

Service Level Agreement (SLA): element of a formal, negotiated commercial contract between two Organizations, i.e. one with a Service Provider (SP) Role and one a Customer Role

NOTE 1: It documents the common understanding of all aspects of the Product and the roles and responsibilities of both Organizations from product ordering to termination.

NOTE 2: This definition is from [i.3].

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

BRR	Basic Return Rate
CSC	Cloud Service Customer
CSP	Cloud Service Provider
CSP:NP	Cloud Service Provider:Network Provider
DOA	Dead On Arrival
DPM	Defects Per Million
EM	Element Manager
EPC	Evolved Packet Core
EPO	Emergency Power Off
ERI	Early Return Index
ESD	Electro-Static Discharge
FCAPS	Fault Configuration Accounting Performance Security
FRT	Fix Response Time
IP	Internet Protocol
IP-TV	Internet Protocol Television
KQI	Key Quality Indicator
LTR	Long-term Return Rate
MANO	Management and Orchestration
MOP	Method of Procedure
NFV	Network Function Virtualisation
NFVI	NFV Infrastructure
NFVO	NFV Orchestrator
NPR	Number of Problem Reports

OFR	Overdue Fix Responsiveness
OSS	Operation Support System
OTD	On Time Delivery
OTS	On-Time Service delivery
PNF	Physical Network Function
RTP	Real-Time Protocol
SFQ	Software Fix Quality
SLA	Service Level Agreement
SO	Service Outage
SONE	Network Element Impact Outage
SP	Service Provider
SPR	Software Problem Report
SQ	Service Quality
SSO	Support Service caused Outages
VIM	Virtual Infrastructure Management
VM	Virtual Machine
VN	Virtual Network
VNF	Virtualised Network Function
VNFC	Virtualised Network Function Component
VNFM	VNF Manager
VoLTE	Voice over Long Term Evolution
YRR	one-Year Return Rate

4 Roles in the NFV Ecosystem

4.1 NFV Service Delivery Relationships

In the present document, an NFV cloud service customer is defined as a party having business relationships for using NFV infrastructure, management and orchestration services [i.9]. Figure 1 illustrates an example of an application service delivery relationship of an NFV cloud service customer following the customer/provider style of [i.3] and using roles from [i.1] and [i.2]. Figure 1 shows NFV Infrastructure, NFV management and orchestration and Functional component offered as a service being provided by a single cloud service provider (CSP) organization, but different organizational arrangement are also considered in the present document. Each of the cloud service customer's providers/suppliers (e.g. NFV infrastructure cloud service provider) may be customers of other suppliers; for example, a cloud service provider who offers NFV infrastructure-as-a-service to NFV cloud service customers (i.e. an NFV Infrastructure cloud service provider is a customer of suppliers of physical compute, networking and storage hardware, various software products and so on).

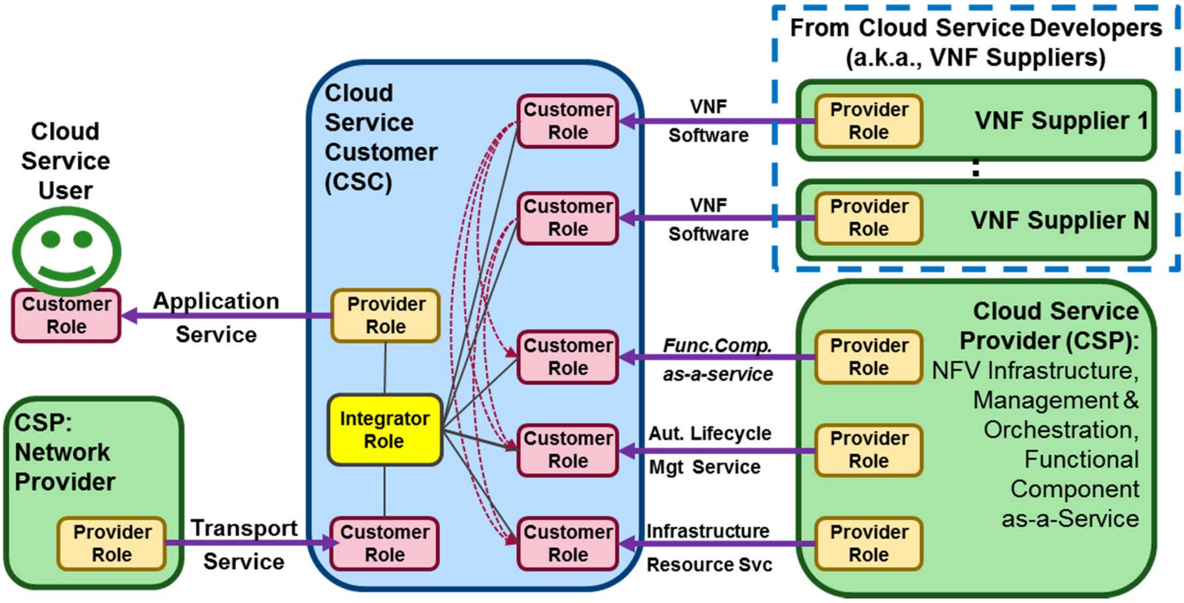


Figure 1: Example of an NFV Service Delivery Relationship for Cloud Service Customer

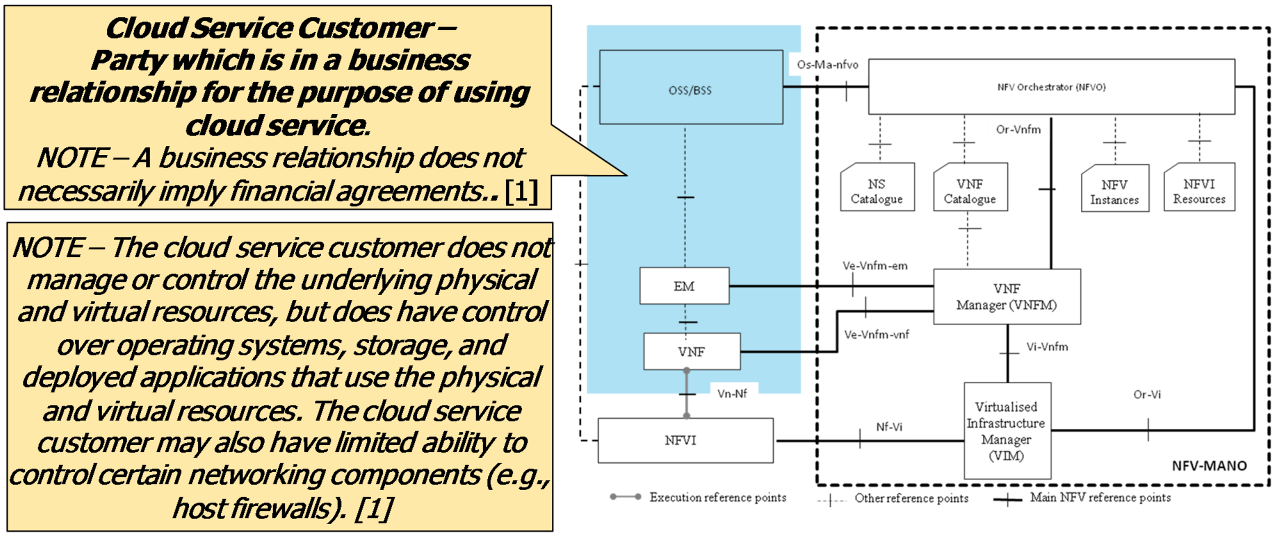
4.2 Role: Cloud Service User

Cloud Service Users are defined by [i.1] as the end users, or applications operating on their behalf, who use cloud services. In the context of NFV, a cloud service user refers to a natural person, or system/device acting on their behalf, that consumes services offered by a cloud service provider. For example, a cloud service user utilizes their smartphone to consume services Voice-over-LTE offered by an NFV cloud service customer.

4.3 Role: Cloud Service Customer

As shown in Figure 2**, Cloud Service Customer** (CSC) is a role that is responsible for operation of a network services for cloud service users to consume. In the context of NFV, a cloud service customer might operate a VNF-based network service like Voice-over-LTE, IP-TV or an evolved packet core that serves cloud service (a.k.a. end) users.

NOTE 1: In the context of TM Forum, a cloud service customer might be a provider of a digital service.

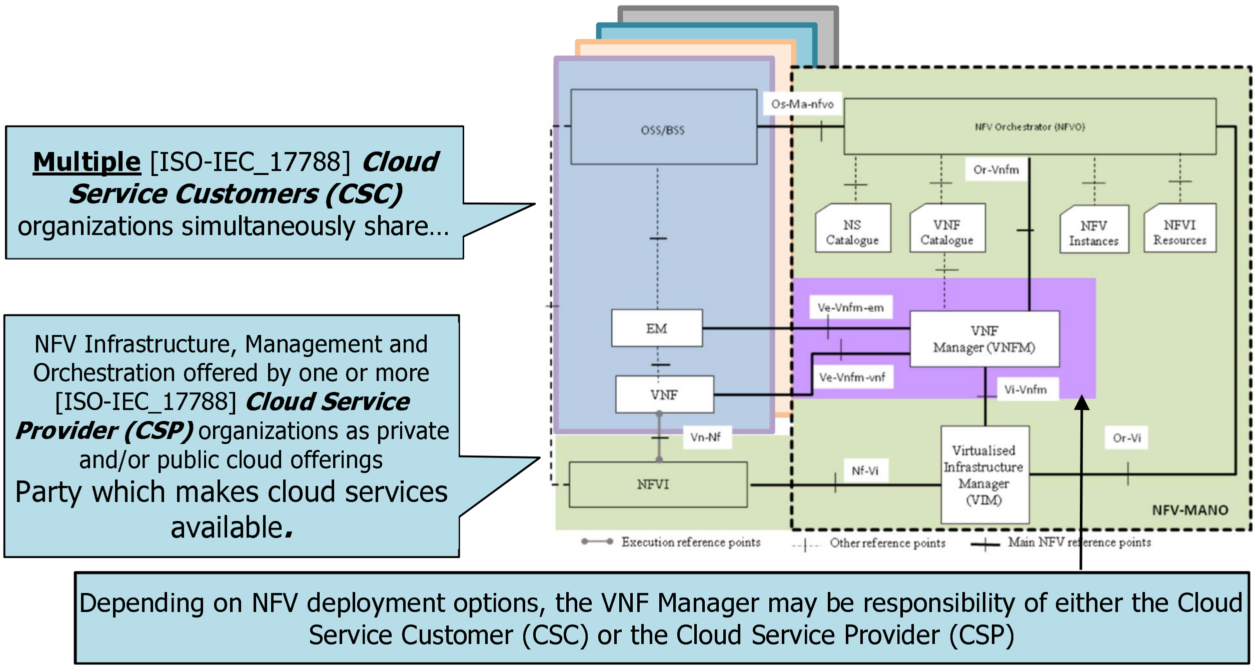


Cloud Service Customer – Party which is in a business relationship for the purpose of using cloud service.
NOTE – A business relationship does not necessarily imply financial agreements.. [1]

NOTE – The cloud service customer does not manage or control the underlying physical and virtual resources, but does have control over operating systems, storage, and deployed applications that use the physical and virtual resources. The cloud service customer may also have limited ability to control certain networking components (e.g., host firewalls). [1]

Figure 2: Cloud Service Customer Role in NFV

Figure 3 illustrates the practical implications of multi-tenancy in NFV: multiple (ISO-IEC 17788) **Cloud Service Customer** organizations are likely to share a public or private NFV infrastructure, management and orchestration cloud which enables each cloud service customer to efficiently offer VNF-based network services like VoLTE, EPC and IP-TV to their respective end users. A single public or private (ISO-IEC 17788) **Cloud Service Provider** organization offers NFV infrastructure, management and orchestration services to all of these cloud service customers.



Multiple [ISO-IEC_17788] ***Cloud Service Customers (CSC)*** organizations simultaneously share…

NFV Infrastructure, Management and Orchestration offered by one or more [ISO-IEC_17788] ***Cloud Service Provider (CSP)*** organizations as private and/or public cloud offerings Party which makes cloud services available.

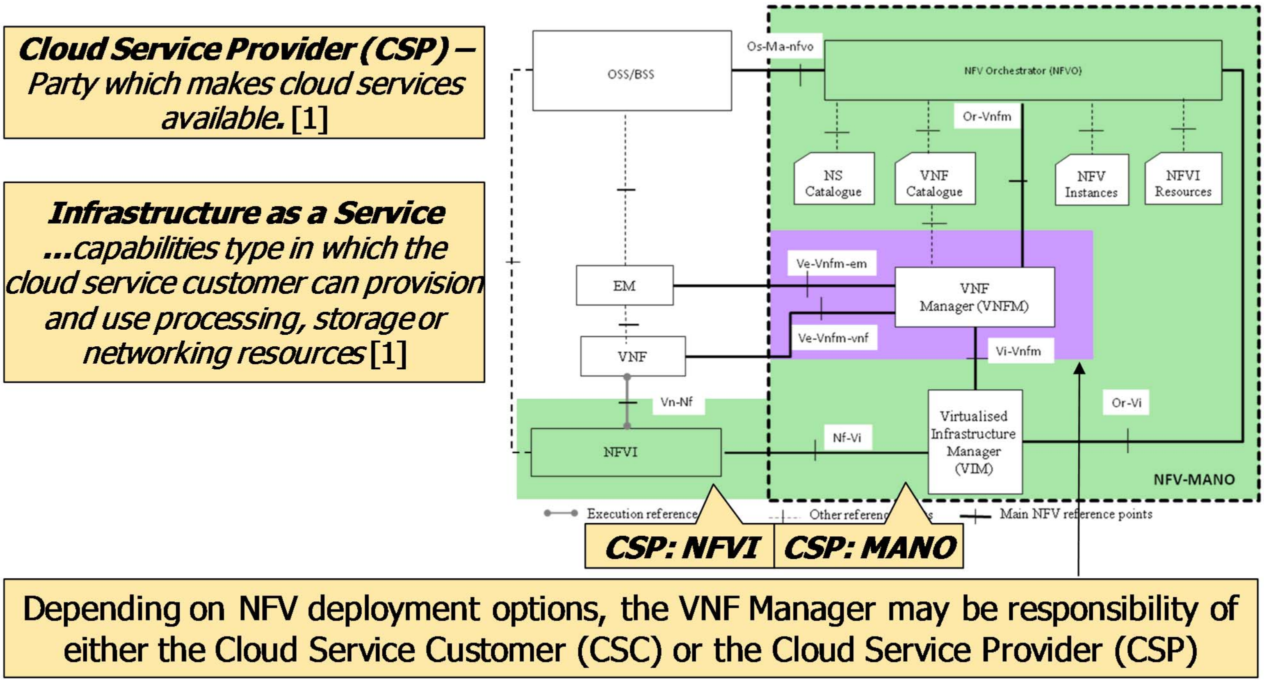
Depending on NFV deployment options, the VNF Manager may be responsibility of either the Cloud Service Customer (CSC) or the Cloud Service Provider (CSP)

Figure 3: Multi-Tenancy in NFV

NOTE 2: This figure is illustrative and the position of the VNF Manager within the MANO scope is only one of the implementation options explored by the ETSI NFV IFA Working Group.

4.4 Role: Cloud Service Provider

As shown in Figure 4**, Cloud Service Provider** (CSP) is broadly defined by [i.1] as a "*Party which makes cloud services available*". In the context of NFV one or more cloud service provider organizations will offer infrastructure, management and orchestration services to cloud service customers, in order to host instances of VNFs that support cloud service customers' users. Cloud service provider organizations may also offer services like load balancing via functional component as-a-Service offerings.



Cloud Service Provider (CSP) – Party which makes cloud services available. [1]

Infrastructure as a Service …capabilities type in which the cloud service customer can provision and use processing, storage or networking resources [1]

CSP: NFVI ***CSP: MANO***

Depending on NFV deployment options, the VNF Manager may be responsibility of either the Cloud Service Customer (CSC) or the Cloud Service Provider (CSP)

Figure 4: Cloud Service Provider Role in NFV

NOTE 1: This figure is illustrative and the position of the VNF Manager within the MANO scope is only one of the implementation options explored by the ETSI NFV IFA Working Group.

Four different primary cloud service provider (sub)roles in the NFV ecosystem are presented in Figure 4:

1) **Cloud Service Provider: NFV Infrastructure** (CSP:NFVI) - the organization that makes virtualised compute, memory, storage and networking resources offered by NFV infrastructure available to cloud service customers, and CSP: Management and Orchestration party if that organization is distinct from the CSP:NFVI organization. Note that ownership and operation of the VIM may be responsibility of the NFV Infrastructure Cloud Service Provider.

2) **Cloud Service Provider: NFV Management and Orchestration** (CSP:MANO) - the organization that makes NFV management and orchestration services available to cloud service customers. A single organization typically offers both CSP:NFVI and CSP:MANO services to cloud service customer organizations, but they may not be the same (e.g. in hybrid cloud or brokered service arrangements). This role is covered by [i.1] ***Cloud Provider***. Note that NFV Management and Orchestration are often served by the same organization serving the NFV Infrastructure that, but some federated, brokered or hybrid arrangements might have a CSP:MANO organization controlling a different CSP:NFVI organization's virtualised resources.

NOTE 2: CSP:NFVI and CSP:MANO could be provided by a single or different organizations. The existing MANO architecture does not consider there could be more than one MANO service provider.

3) **Cloud Service Provider: Functional Component** (CSP:FC) - According to [i.2] "*a **functional component** is a functional building block needed to engage in an activity, backed by an implementation*". For instance, a database or load balancer is a functional component that a cloud service provider can offer as-a-Service to cloud service customers.

4) **Cloud Service Provider: Network Provider** (CSP:NP) - The CSP:network provider provides transport connectivity between cloud data centres and from cloud data centres to cloud service users. Clause B.7 Functional Components Offered as-a-Service illustrates a typical CSP:NP use case scenario.

NOTE 3: Role (3) and (4) might not be part of the NFV architecture.

4.5 Role: VNF Supplier

VNF Suppliers are cloud service developers who provide and support VNFs as products to cloud service customers or cloud service providers. Note that VNF Supplier can also be referred to as VNF Provider.

4.6 Role: Service Integrator

Network services can be implemented as service chains composed of multiple VNFs from different VNF suppliers integrated with various functional components offered as-as-Service, and perhaps instantiated across NFVI in several geographically distributed cloud data centres. Cloud service customers and providers can contract some or all of this integration and testing of service chains and VNFs to parties offering integration and testing as a professional service. In such case, it is important to recognize the responsibility and accountability boundaries between the VNF suppliers, the functional components offered-as-a-Service and the integrator who brings those offers together into a valuable service. It is also important to clarify the responsibility and accountability boundary between (often one-time) service integrator and the cloud service customer's team who operate the production service on a routine basis. Implementation of a network service might involve several service integrators who put together and test various service chains and functionality, all of which may be coordinated by the cloud service customer or provider, or by another service integrator acting as a prime contractor. The Cloud Service Customer can be the sole service integrator.

Operationally, cloud service customers or providers might contract service integrators to take accountability for addressing specific problems of some network service or offering, such as determining an optimal capacity management policy to assure that sufficient spare online capacity to serve lead time demand, random variations and unforecast surges in demand, and mitigate user service impact of failure events. Clear accountabilities and responsibilities of VNF suppliers, service integrators, cloud service providers and the cloud service customer both minimizes the risk of errors at those organizational boundaries and enables rapid fault localization when failures inevitably occur.

4.7 Role: Cloud Auditor

Cloud Auditor conducts audits against agreed specifications, policies and agreements, such as information security audits against ISO/IEC 27001 [i.16] and performance audits against the terms of a service level agreement. Auditors from other organizations may be used to independently verify compliance to specifications, policies and agreements; for example a cloud service customer may arrange for an independent organization to audit a cloud service provider, VNF supplier or service integrator.

4.8 Role: Cloud Service Broker

Cloud Service Broker (not shown in Figure 1) may be involved in arranging end-to-end service chains across multiple cloud service providers to meet cloud service customers' needs, but not in actual service delivery.

4.9 Illustrative Example

While some private cloud service providers will supply integrated NFV infrastructure, management, orchestration and functional components offered as-a-service to cloud service customers, other deployments will unbundle these cloud services. Figure 5 shows a sample configuration of the deployment model of Figure 1 with the following roles:

- **NFV Infrastructure Cloud Service Provider (CSP:NFVI)** - one or more organizations operate cloud data centres to support the cloud service users (a.k.a. customers) of their cloud service customer's end users, such as a small cloud infrastructure deployment in a central office or base station that is physically very close to some cloud service users.

- **Management and Orchestration Cloud Service Provider** (CSP:MANO) - the organization that offers management and orchestration services to the cloud service customer that supports VNF deployment across myriad small cloud data centres. The CSP:MANO cloud service provider organization may be the same as the CSP:NFVI organization.

- **Functional Component offered as-a-Service Cloud Provider** (CSP:FC) - one or more organizations may offer functional-components as-a-service to the cloud service customer.

- **VNF Suppliers** offer VNF packages to the cloud service customer.

- **Service Integrators** offer integration and testing of services, and professional/consulting services to cloud service customers and providers. These services may cover integrating multiple VNFs into a network service and/or integrating VNFs with one or more functional-components-offered-as-a-service as well as with the target CSP:MANO and CSP:NFVI offerings (indicated by dotted arrows in Figure 5).

- **Network Providers (CSP:NP)** offer network connectivity between cloud service users and NFV infrastructure cloud service provider's data centres.

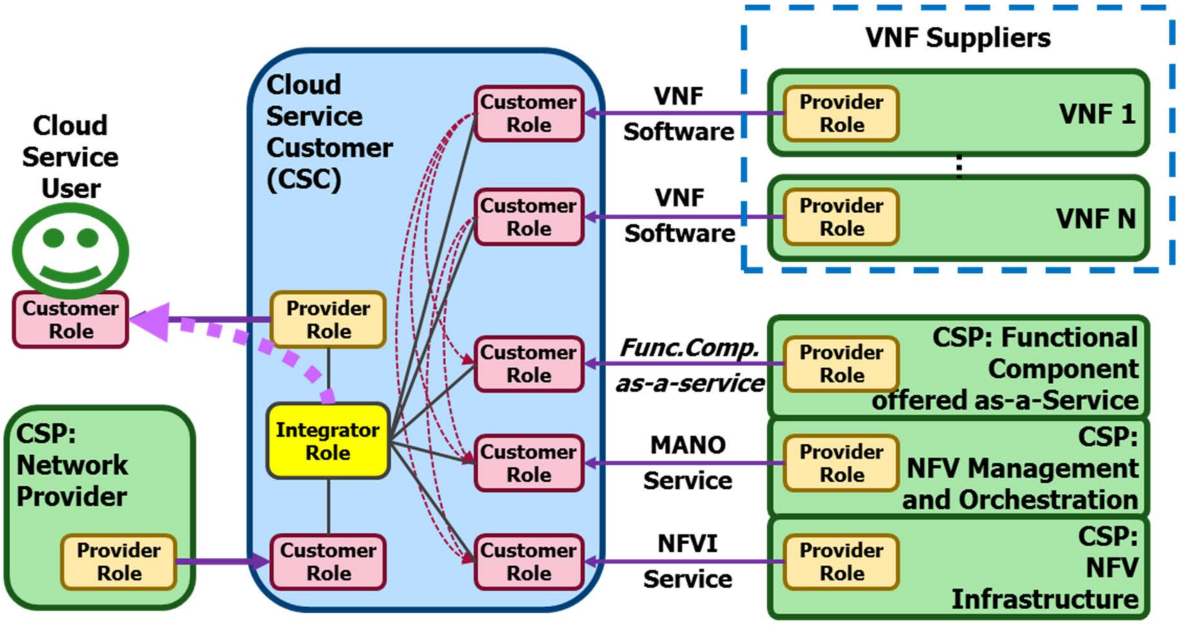


Figure 5: Sample Deployment Model

Figure 6 shows an example of how these roles fit into the quality accountability framework at the highest level for a simple, hypothetical TL 9000 product category 6.1 voice mail server. The quality of voice mail service experienced by cloud service (end) users of the cloud service provider's offering is driven by:

- **Quality of VNF software delivered by the supplier** of the voice mail application. For example, if the voice mail software is buggy, then end users may experience poor service quality.

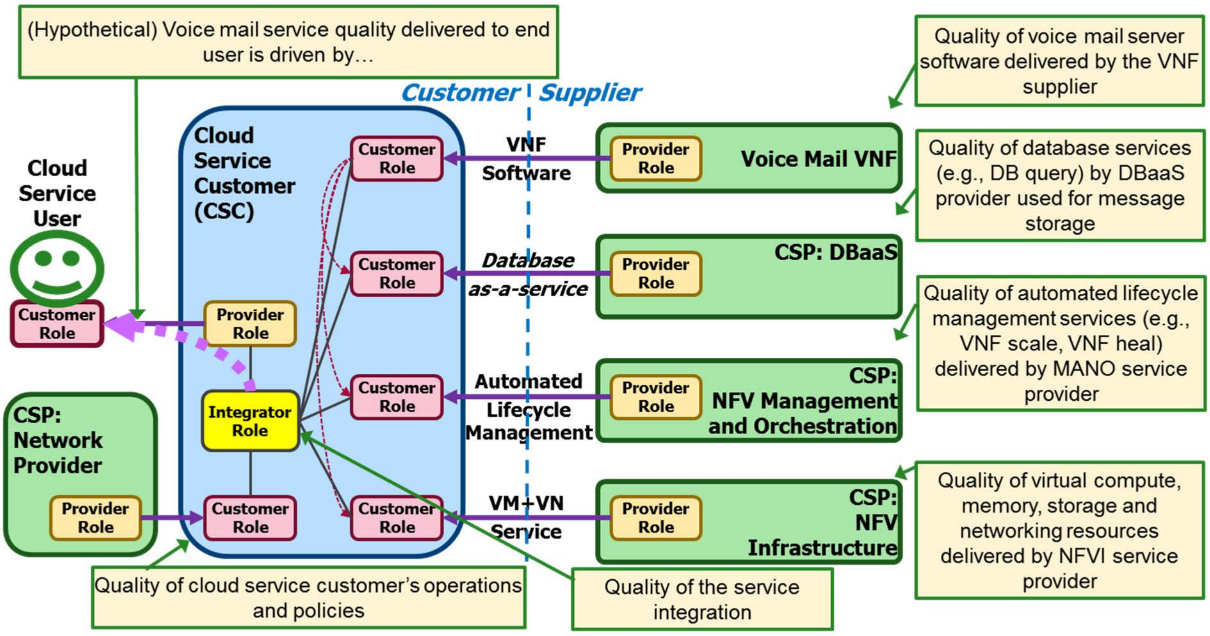
- **Quality of the database-as-a-service that the cloud service customer selected and integrated** as the backend data repository for the voice mail system. For example, if the backend database hosting voice mail messages is unavailable or unreliable, then end users may experience poor service quality.

- **Quality of the automated lifecycle management services delivered by the NFV management and orchestration service provider when fulfilling the cloud service customer's requests** to VNF scale, VNF heal, VNF update and so on. For example, if the MANO provider cannot reliably complete VNF (growth) scale actions when promised, then insufficient application capacity may be online to serve all end user workload with acceptable service quality.

- **Quality of the virtual compute, memory, storage and networking resources delivered by the NFVI service provider**. For example, bursts of network packet loss may cause poor quality voice recordings to be captured in the database, so end users endure low quality voice messages.

- **Quality of the service integration**. Integration of VNF packages to build a network service involves interactions with NFV infrastructure, management and orchestration, functional components and will likely include development, testing and optimization of numerous configurations, scripts, descriptor files, operational policies and manual procedures. Cloud service providers may subcontract various aspects of service integration to their VNF suppliers, cloud service providers and/or professional service integrators. As network service integration often cuts across at least one VNF and at least one cloud service provider, errors across those organizational and service boundaries are always possible. For example, how effectively automated lifecycle management failures are detected and mitigated.

- **Quality of the cloud service customer's operations and polices**. Cloud service customers will establish operational policies ranging from training and experience required by their operations staff, to how quickly problems are escalated to their VNF suppliers and cloud service providers, to how and when forecasts of user demand are made. For example, if the cloud service customer's operational policies are too lean and they fail to maintain sufficient reserve application capacity online, then an extreme spike in user demand that exhausts online reserve capacity will cause some users to experience poor service quality, or perhaps to even be denied service.



(Hypothetical) Voice mail service quality delivered to end user is driven by…
Customer
Supplier
Quality of voice mail server software delivered by the VNF supplier
Cloud Service User
Customer Role
Cloud Service Customer (CSC)
Customer Role
Customer Role
Customer Role
Customer Role
Customer Role
Provider Role
Integrator Role
VNF Software
Database as-a-service
Automated Lifecycle Management
VM+VN Service
Provider Role
Voice Mail VNF
Provider Role
CSP: DBaaS
Provider Role
CSP: NFV Management and Orchestration
Provider Role
CSP: NFV Infrastructure
Quality of database services (e.g., DB query) by DBaaS provider used for message storage
Quality of automated lifecycle management services (e.g., VNF scale, VNF heal) delivered by MANO service provider
Quality of virtual compute, memory, storage and networking resources delivered by NFVI service provider
CSP: Network Provider
Provider Role
Quality of cloud service customer's operations and policies
Quality of the service integration

Figure 6: Hypothetical Quality Accountabilities

Clarifying the roles, responsibilities and quantitative service objectives across each of these customer:supplier service boundaries enables efficient engineering, operations, fault localization, root cause analysis and corrective actions.

5 Responsibilities by Role

5.1 Traditional (PNF) Responsibilities

The core responsibility model of the traditional (i.e. PNF) telecom ecosystem can be summarized as follows: service providers purchase and operate equipment from suppliers to deliver services to end users. Responsibilities are standardized via [i.5] which factored outages into three categories for attribution:

- **Product attributable outage** - An outage primarily triggered by
    - the system design, hardware, software, components or other parts of the system;
    - scheduled outage necessitated by the design of the system;
    - support activities performed or prescribed by an organization including documentation, training, engineering, ordering, installation, maintenance, technical assistance, software or hardware change actions, etc.;
    - procedural error caused by the organization;
    - the system failing to provide the necessary information the to conduct a conclusive root cause determination; or
    - one or more of the above [i.5].
- **Customer** (e.g. service provider) **attributable outage** - An outage that is primarily attributable to the customer's equipment or support activities triggered by:
    - customer procedural errors;
    - office environment, for example power, grounding, temperature, humidity, or security problems; or
    - one or more of the above.

  Outages are also considered customer attributable if the customer refuses or neglects to provide access to the necessary information for the organization to conduct root cause determination [i.5].
- **External attributable outage** - Outages caused by natural disasters such as tornadoes or floods, and outages caused by third parties not associated with the customer or the organization such as commercial power failures, third-party contractors not working on behalf of the organization or customer [i.5].

In this model, each (PNF) supplier organization is accountable for outages attributed to products provided by the supplier; the service provider is accountable for integrating PNFs into a service as well as their customer attributable outages and mitigating external attributable outages.

5.2 VNF Supplier Responsibilities

VNF supplier is responsible for:

- Quality and correctness of VNF design and software.
- Quality and correctness of documentation, training, technical assistance of the VNF.
- Quality and correctness of scripts, files and other materials supporting automated lifecycle management provided by the VNF supplier.
- Scheduled outages necessitated by the design of the VNF.
- Support activities performed by the VNF supplier.

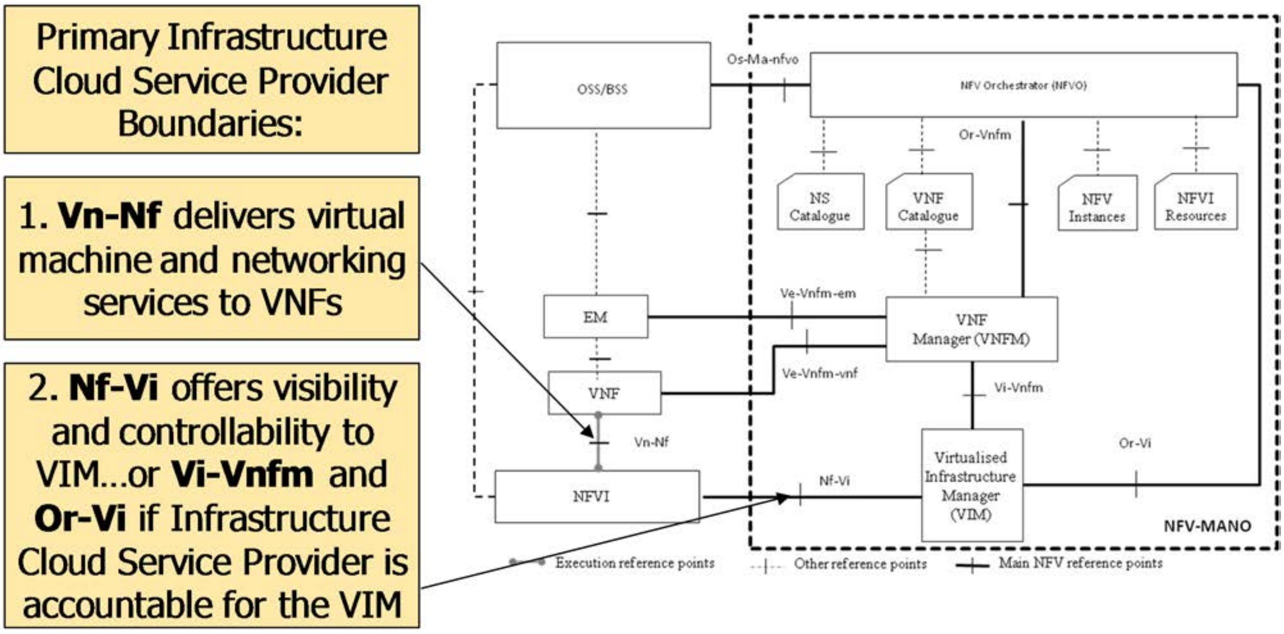
5.3 Service Integrator Responsibilities

Service integrators' responsibility is tied to the specific activities that the cloud service customer or cloud service provider ordered them to accomplish. In some engagements, a service integrator might be responsible for integrating one or more VNFs with zero or more functional component as-a-Service offerings. In other engagements a service integrator might be responsible for preparing VNF and network service descriptors and scripts. In yet another engagement the integrator might be responsible for developing policies like determining the criteria and algorithms for VNF and network service scaling. As with any other reputable supplier serving a cloud service customer or cloud service provider, service integrators take accountability for the accuracy, correctness, performance and delivery schedule adherence of their work products.

5.4 Cloud Service Provider: NFV Infrastructure

As shown in Figure 7, the infrastructure cloud service provider organizations expose two primary service interfaces:

- Vn-Nf delivers virtual machine and virtual networking services to VNFC instances of VNFs hosted on the infrastructure.
- Nf-Vi offers management visibility and controllability to authorized Virtualised Infrastructure Manager when the NFV management and orchestration service provider organization(s) is accountable for the VIM. If the infrastructure cloud service provider is accountable for the VIM, then the infrastructure visibility and controllability for the NFV management and orchestration service provider organization is across both the Vi-Vnfm and Or-Vi reference points.



Primary Infrastructure Cloud Service Provider Boundaries:

1. **Vn-Nf** delivers virtual machine and networking services to VNFs

2. **Nf-Vi** offers visibility and controllability to VIM...or **Vi-Vnfm** and **Or-Vi** if Infrastructure Cloud Service Provider is accountable for the VIM

Figure 7: Primary Infrastructure Cloud Service Provider Boundaries

The Infrastructure cloud service provider organization is responsible for:

- Timely and accurate allocation of virtual machine, networking and storage resources.
- Consistent high quality delivery of virtual compute, memory, storage and networking service to allocated resources.
- Timely and accurate reporting of infrastructure faults and failures.
- Accurate resource usage reporting.
- Data centre environment hosting infrastructure equipment, for example power, grounding, temperature, humidity, or security problems.

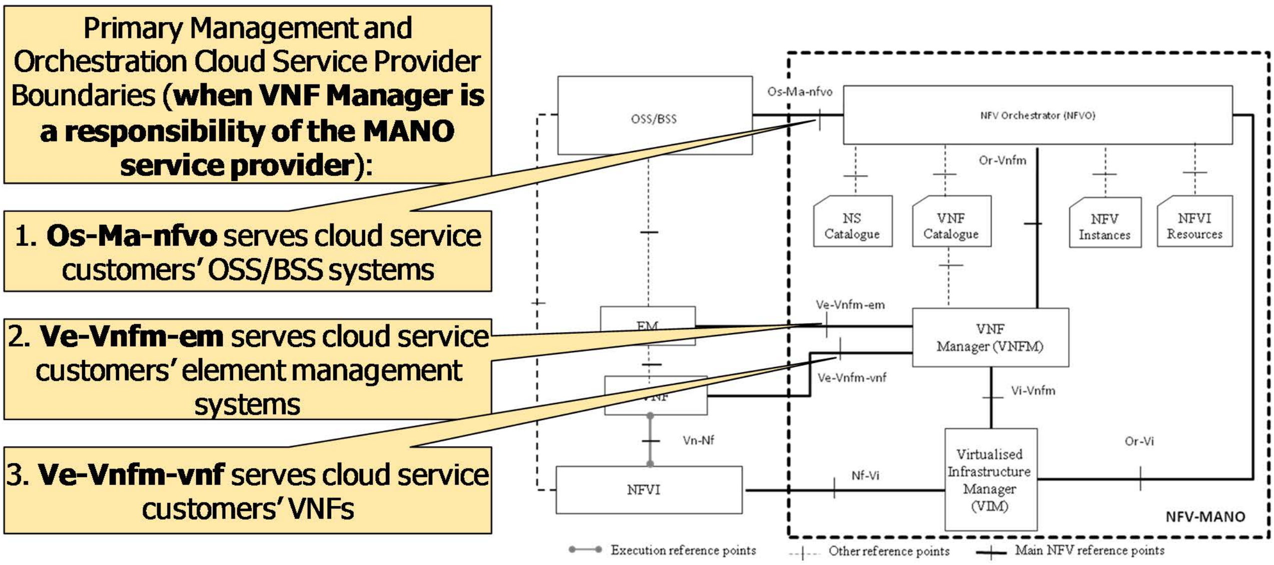
5.5 Cloud Service Provider: NFV Management and Orchestration

As shown in Figure 8, the management and orchestration cloud service provider organizations that are accountable for VNF Managers expose three primary service interfaces to cloud service customers:

1) Os-Ma-nfvo serves cloud service customers' operations support and business support systems (OSS/BSS).

2) Ve-Vnfm-em serve cloud service customers' element management (EM).

3) Ve-Vnfm-vnf serves cloud service customers' VNFs (VNF).



Primary Management and Orchestration Cloud Service Provider Boundaries (**when VNF Manager is a responsibility of the MANO service provider**):

1. **Os-Ma-nfvo** serves cloud service customers' OSS/BSS systems

2. **Ve-Vnfm-em** serves cloud service customers' element management systems

3. **Ve-Vnfm-vnf** serves cloud service customers' VNFs

Figure 8: Primary Management and Orchestration Cloud Service Provider Boundaries (including VNFM)

Figure 9 visualizes the management and orchestration cloud service provider's boundaries when the cloud service customer is responsible for the VNF manager:

- Os-Ma-nfvo serves cloud service customers' operations support and business support systems.
- Or-Vnfm from cloud service customer's VNFM to cloud service provider's NFVO.
- Vi-Vnfm from cloud service customer's VNFM to cloud service provider's VIM.

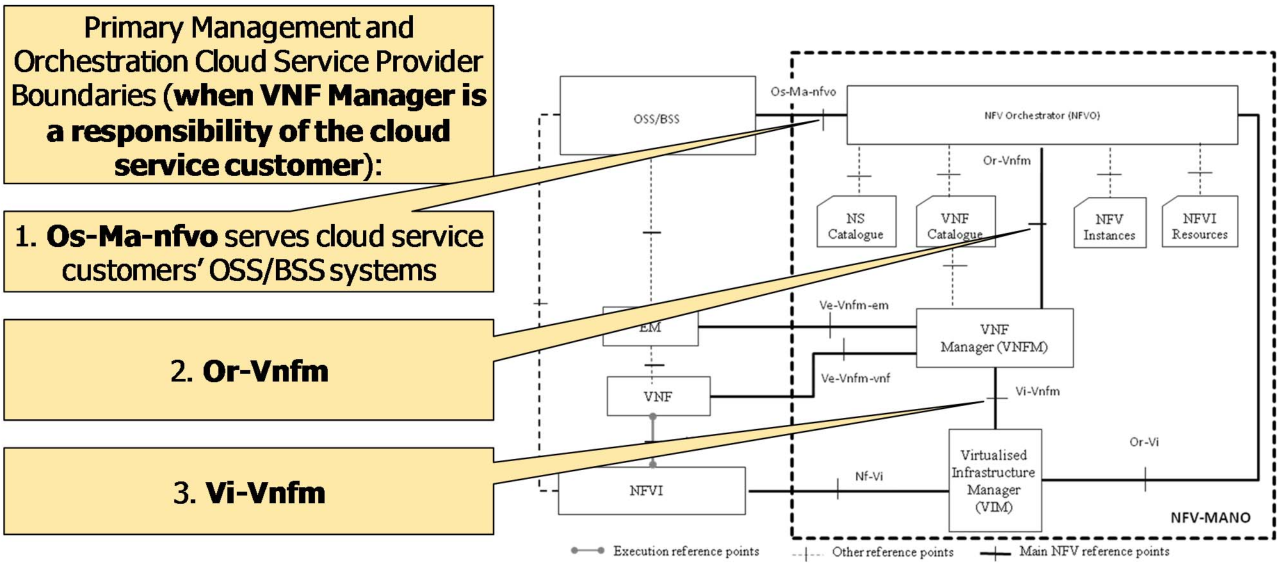

Primary Management and Orchestration Cloud Service Provider Boundaries (**when VNF Manager is a responsibility of the cloud service customer**):
1. **Os-Ma-nfvo** serves cloud service customers' OSS/BSS systems
2. **Or-Vnfm**
3. **Vi-Vnfm**
OSS/BSS
Os-Ma-nfvo
NFV Orchestrator (NFVO)
Or-Vnfm
NS Catalogue
VNF Catalogue
NFV Instances
NFVI Resources
EM
Ve-Vnfm-em
VNF Manager (VNFM)
VNF
Ve-Vnfm-vnf
Vi-Vnfm
Or-Vi
NFVI
Nf-Vi
Virtualised Infrastructure Manager (VIM)
NFV-MANO
Execution reference points
Other reference points
Main NFV reference points

Figure 9: Primary Management and Orchestration Cloud Service Provider Boundaries (excluding VNFM)

The cloud management and orchestration service provider organization is responsible for:

1) Timely and accurate execution of lifecycle management actions requested by the cloud service customers.

2) Timely and accurate execution of cloud service customers' network forwarding graph and network service lifecycle management and orchestration actions.

3) Timely and accurate virtual resource management and orchestration.

4) Timely and accurate enforcement of management and orchestration policies, including cloud service customers' anti-affinity rules.

5) Timely and accurate reporting of network service, VNF and resource faults.

5.6 Cloud Service Provider: Functional Component Offered as-a-Service

The cloud functional component as-a-service provider organization is responsible for:

1) Assuring that the functional component service capacity is at least as available, reliable and responsive to the cloud service customer as agreed in service level objectives.

2) Offering available, reliable and responsive on-demand self-service functional component configuration to the cloud service customer.

3) Accurate functional component usage recording.

4) Timely and accurate reporting of functional component faults.

5.7 Cloud Service Customer

The cloud service customer organization is responsible for:

1) Overall (e.g. end-to-end) service quality experienced by the cloud service users.

2) Integration of VNF instances with the cloud service customer's preferred infrastructure, management, orchestration and functional component as-a-service provider(s).

3) Architecture, configuration and operational policies (e.g. thresholds to trigger scaling actions) of VNF (and PNF) service chains to meet cloud service users' quality expectations, provided VNF suppliers, cloud infrastructure, management, orchestration and functional component service providers meet their agreed service quality objectives.

4) Mitigation of force majeure and other external attributable incidents.

5) Fault isolation and root cause analysis of service failures.

5.8 CSP: Network Provider

Responsibilities of cloud network service provider organization are not detailed in the present document.

6 Responsibilities for Key Cloud Characteristics

6.1 Key Cloud Computing Characteristics

The highest level responsibilities of the roles of the previous clause are understood by considering their responsibilities in the context of the six key characteristics of cloud computing given in clause 6.2 of [i.1].

6.2 Broad Network Access

ISO/IEC 17788 [i.1] defines the **broad network access** key characteristic of cloud computing as follows:

*"A feature where the physical and virtual resources are available over a network and accessed through standard mechanisms that promote use by heterogeneous client platforms. The focus of this key characteristic is that **cloud computing** offers an increased level of convenience in that users can access physical and virtual resources from wherever they need to work, as long as it is network accessible, using a wide variety of clients including devices such as mobile phones, tablets, laptops, and workstations;".*

a) The CSP:network provider has responsibility for broad network access.

6.3 Measured Service

ISO/IEC 17788 [i.1] defines the **measured service** key characteristic of cloud computing as follows:

*"A feature where the metered delivery of **cloud services** is such that usage can be monitored, controlled, reported, and billed. This is an important feature needed to optimize and validate the delivered **cloud service**. The focus of this key characteristic is that the customer may only pay for the resources that they use. From the customers' perspective, **cloud computing** offers the users value by enabling a switch from a low efficiency and asset utilization business model to a high efficiency one;".*

a) Each cloud service provider (CSP) has responsibility for measured services of their offering to cloud service customers (CSCs).

b) Each cloud service customer (CSC) has responsibility for measured services of their offering to cloud service users.

6.4 Multi-Tenancy

ISO/IEC 17788 [i.1] defines the **multi-tenancy** key characteristic of cloud computing as follows:

*"A feature where physical or virtual resources are allocated in such a way that multiple **tenants** and their computations and data are isolated from and inaccessible to one another. Typically, and within the context of **multi-tenancy**, the group of **cloud service users** that form a **tenant** will all belong to the same **cloud service customer** organization. There might be cases where the group of **cloud service users** involves users from multiple different **cloud service customers**, particularly in the case of **public cloud** and **community cloud** deployments. However, a given **cloud service customer** organization might have many different tenancies with a single **cloud service provider** representing different groups within the organization;".*

a) Cloud service provider (CSP) has responsibility for assuring that agreed service quality delivered to cloud service customers (CSCs) is not impacted by any other tenants.

b) Cloud service customers (CSCs) have responsibility for assuring that agreed service quality to one cloud service user is not impacted by other cloud service users of the cloud service customer's service offering.

6.5 On-Demand Self Service

ISO/IEC 17788 [i.1] defines the **on-demand self-service** key characteristic of cloud computing as follows:

*"A feature where a **cloud service customer** can provision computing capabilities, as needed, automatically or with minimal interaction with the **cloud service provider**. The focus of this key characteristic is that **cloud computing** offers users a relative reduction in costs, time, and effort needed to take an action, since it grants the user the ability to do what they need, when they need it, without requiring additional human user interactions or overhead;".*

a) Each cloud service provider (CSP) has responsibility for assuring the quality of on-demand self service capabilities that are offered to cloud service customers (CSCs).

6.6 Rapid Elasticity and Scalability

ISO/IEC 17788 [i.1] defines the **rapid elasticity and scalability** key characteristic of cloud computing as follows:

*"A feature where physical or virtual resources can be rapidly and elastically adjusted, in some cases automatically, to quickly increase or decrease resources. For the **cloud service customer**, the physical or virtual resources available for provisioning often appear to be unlimited and can be purchased in any quantity at any time automatically, subject to constraints of service agreements. Therefore, the focus of this key characteristic is that **cloud computing** means that the customers no longer need to worry about limited resources and might not need to worry about capacity planning;".*

a) Each cloud service provider (CSP) has responsibility for assuring rapid elasticity and scalability of the resources and functional components that they offer as-a-service to cloud service consumers within pre-defined limits.

b) Each VNF supplier has responsibility for assuring that their VNFs support rapid elasticity and scalability within agreed limits.

c) Each cloud service customer has responsibility for assuring that automated lifecycle management arrangements, trigger thresholds and policies are configured to meet their capacity needs while remaining within the agreed scaling limits of the cloud service providers' resources, lifecycle management mechanisms and functional components offered as-a-service as well as VNF limits stipulated by VNF suppliers.

6.7 Resource Pooling

ISO/IEC 17788 [i.1] defines the **resource pooling** key characteristic of cloud computing as follows:

*"A feature where a **cloud service provider's** physical or virtual resources can be aggregated in order to serve one or more **cloud service customers**. The focus of this key characteristic is that **cloud service providers** can support **multi-tenancy** while at the same time using abstraction to mask the complexity of the process from the customer. From the customer's perspective, all they know is that the service works, while they generally have no control or knowledge over how the resources are being provided or where the resources are located. This offloads some of the customer's original workload, such as maintenance requirements, to the provider. Even with this level of abstraction, it should be pointed out that users might still be able to specify location at a higher level of abstraction (e.g. country, state, or data centre).".*

a) Each cloud service provider (CSP) has responsibility for all agreed aspects of operation, administration, maintenance and assurance of the resources they offer to cloud service customers (CSCs).

b) Cloud service consumers (CSCs) are responsible for all agreed aspects of operations, administration, maintenance, provisioning and assurance of services they provide to cloud service users.

7 Quality Measurement Framework

7.1 Overview

The NFV quality accountability framework integrates three pieces:

1) **Roles**, covered in clause 4 *Roles in the NFV Ecosystem*.

2) **Responsibilities**, covered in clauses 5 *Responsibilities by Role* and 6 *Responsibilities for Key Cloud Characteristics*.

3) **Service quality measurements and demarcation points**, which are visualised in Figure 10.

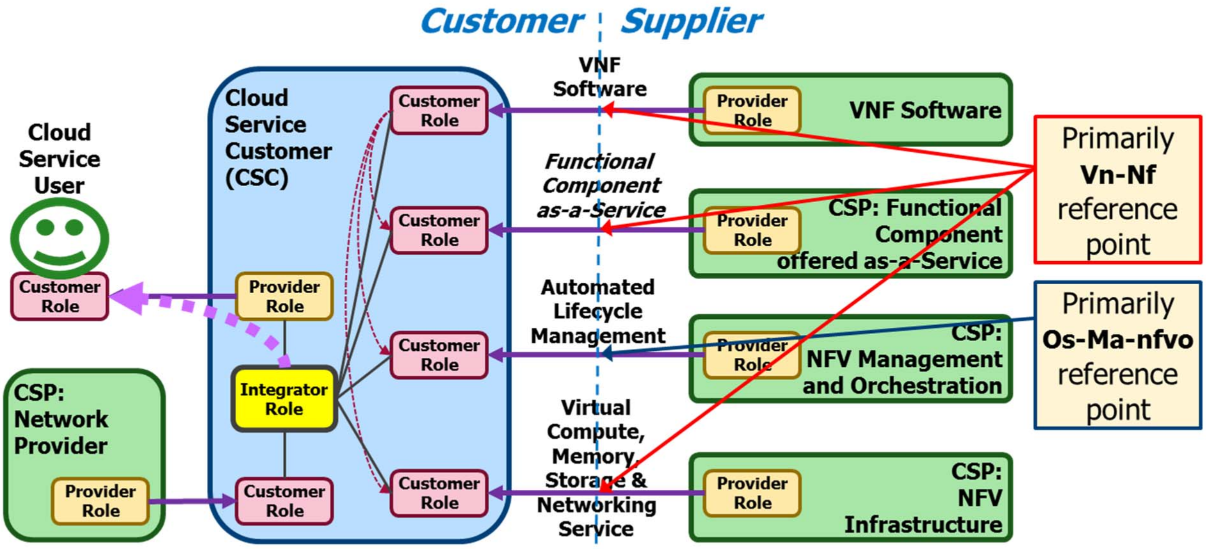

Customer
Supplier
Cloud Service User
Customer Role
CSP: Network Provider
Provider Role
Cloud Service Customer (CSC)
Customer Role
Customer Role
Provider Role
Integrator Role
Customer Role
Customer Role
Customer Role
VNF Software
Functional Component as-a-Service
Automated Lifecycle Management
Virtual Compute, Memory, Storage & Networking Service
Provider Role
VNF Software
Provider Role
CSP: Functional Component offered as-a-Service
Provider Role
CSP: NFV Management and Orchestration
Provider Role
CSP: NFV Infrastructure
Primarily Vn-Nf reference point
Primarily Os-Ma-nfvo reference point

Figure 10: NFV Service Quality Measurements

7.1 VNF Software Quality Measurements

The quality of VNF software is objectively and quantitatively measured via TL 9000 measurements:

- **Outage Downtime (SO, SONE)** - [i.5], clause 6 details outage metrics; those primarily applicable to the NFV quality measurement framework are:

  - **Service Impact Outage** (SO) The Service Impact Outage measurements guide organizations and customers in assessing the impact of **outages on the end-user service**. These measurements provide insight into the primary function availability of the product (see [i.5], clause 6.1.1).

  - **Network Element Impact Outage (SONE)** The Network Element Impact Outage measurements guide organizations and customers to effectively manage the costs required to maintain and service the product. Due to product configuration, network resiliency and network element redundancy, **not all outages reported in these measurements cause the loss of service to an end user**. However, each outage results in a maintenance effort for the customer and thereby impacts operation and maintenance costs (see [i.5], clause 6.2.1).

General outage measurement rules from [i.5], clause 6 are supplemented with product-category-specific outage measurement rules from Table A-3 of [i.5] which stipulate how outage downtime is measured slightly differently for, say, a media gateway ([i.5] product category 1.2.3) or a home location register ([i.5] product category 2.3) or an element management system ([i.5] product category 4.2.1 or 4.2.2). QuEST Forum will provide assurance (1) that product category definitions exist for all NFV architectural elements, such as NFV infrastructure equipment, and (2) that outage measurements and other aspects of [i.5] properly accommodate elastic capacity and other cloud characteristics of [i.1].

- **Number of Problem Reports** ([i.5] NPR) objectively measures the problem report rate. QuEST Forum provides assurance that normalized number of problem reports are applicable to VNFs and all NFV architectural elements.

- **Software Problem Report** ([i.5] SPR) objectively measures the software problem report rate. QuEST Forum provides assurance that software problem reports are applicable to VNFs and all NFV architectural elements.

- **Problem Report Fix Response Time** ([i.5] FRT) measures an organization's overall responsiveness to customer-originated problem reports. QuEST Forum provides assurance that problem report fix responsiveness is applicable to VNFs and all NFV architectural elements.

- **Overdue Problem Report Fix Responsiveness** ([i.5] OFR) measures the responsiveness to customer-originated problem reports that are not fixed on time according to the counting rules for the Fix Response Time measurement. QuEST Forum provides assurance that overdue problem report fix responsiveness is applicable to VNFs and all NFV architectural elements.

- **Software Fix Quality** ([i.5] SFQ) objectively measures the effectiveness of an organization's software fix processes. QuEST Forum provides assurance that software fix quality measurement is applicable to VNFs and all NFV architectural elements.

- **On Time Delivery** ([i.5] OTD) objectively measures timeliness of delivery of products to customers. Note that [i.5], clause 5.4.4.c.2 stipulates: *Software deliveries that are not physically shipped or downloaded by the organization to a customer location are not counted*. Thus, OTD does not apply to VNF (or PNF) software that is downloaded by the customer (a.k.a. pulled). QuEST Forum provides assurance that OTD metrics can be applied to NFV infrastructure equipment, and to NFV software as appropriate per [i.5].

7.2 Function Components Offered as-a-Service Quality Measurements

Quality of functional components offered as a service by cloud service providers is objectively and quantitatively measured via Technology-Component-as-a-Service metrics in [i.6]. Functional components offered as-a-service can also be measured via [i.5] as instances of product category 9.6 "*e-Business and Content Hosting"* which is defined as "*chargeable service products offered separately or as part of a solution to customers with data, Internet/Intranet and information systems needs."*.

7.3 Automated Lifecycle Management Quality Measurements

Quality of manually executed lifecycle management actions like new equipment installation, expansion installation, upgrade installation, maintenance and other services are objectively and quantitatively measured via [i.5] product category 7 "*service products"* measurements. NFV management and orchestration automates execution of lifecycle management jobs, so instead of humans executing a Method of Procedure (MOP), NFV orchestrators, VNF Managers, Virtualised Infrastructure Managers and other elements execute lifecycle management actions automatically. Some important attributes change, like promised completion times for lifecycle management actions shrinking from being measured in days or weeks to being measured in minutes; however many measurements remain relevant, like:

- On time delivery - was lifecycle management completed by the promised time?

- Service quality (SQ), i.e. was the lifecycle management action completed correctly?

- Number of problem reports (NPR).

- Problem report fix response time (FRT).

- Overdue problem report fix responsiveness (OFR).

- Support Service Caused Outage (SSO).

[i.8] details these measurements.

7.4 Failure Notification Quality Measurements

Failure notification latency, reliability and accuracy in [i.1] and orchestration service quality metrics in [i.6] are also useful.

7.5 Virtual Infrastructure Quality Measurements

Quality of virtual compute, memory, storage and networking services offered by NFV infrastructure service providers are measured via virtual machine and virtual networking service quality metrics in [i.6].

Hardware reliability has traditionally been measured via Basic Return Rate (BRR), Early Return Indicator (ERI), Yearly Return Rate (YRR) and Long Term Return Rate (LTR) from [i.5], clause 7. NFV infrastructure equipment may be operated differently from traditional telecommunications hardware, such as treating some compute, networking, storage and memory components as consumable rather than repairable (i.e. field replaceable). Even if NFV infrastructure equipment is consumed rather than repaired, it is important to have objective and quantitative measurements of hardware failure rates so that equipment suppliers and equipment customers have the same expectations for hardware reliability. QuEST Forum provides hardware reliability measurements that are appropriate for NFV infrastructure equipment that is not routinely repaired.

Annex A (informative): Sample Cloud Service Customer SLAs

Per [i.4], "*the Service Level Agreement serves as a means of formally documenting the performance expectations, responsibilities and limits between service providers and their Customers*." [i.4] recognizes three types of service level agreements:

1) Supplier SLAs, such as between a cloud service customer and a public cloud service provider.

2) Operational Level Agreements (OLAs), also known as Internal SLAs, such as between a cloud service customer and their cloud service provider in the context of a private cloud deployment.

3) Implicit SLAs.

Service Level Agreements (SLAs) exist in the context of business service agreements which typically consider:

1) **Stakeholders involved in the ecosystem**; these will be organizations serving in roles defined in clause 4 *Roles in the NFV Ecosystem.*

2) **Regulatory Compliance, Legal** - beyond the scope of this annex.

3) **Remedy and Compensation** - beyond the scope of this annex.

4) **Service Level Specifications (SLSs)** - The technical heart of an SLA is the service level specification which includes:

    - **Key Quality Indicator (KQI)** - a metric capturing some aspect of the product that is important to the customer, such as service outage downtime.

    - **Threshold** - one or more values determining the acceptability of an actual KQI measurement. Thresholds may be simple (e.g. the value separating acceptable performance from unacceptable performance) or there may be gradations (e.g. excellent, very good, good, poor, unacceptable). Actual KQI thresholds for acceptable performance will be set by cloud service customers and their cloud service providers and suppliers, and thus are beyond the scope of this annex.

    - **Measurement Point** - the physical or logical demarcation point between supplier and customer where measurements are to be made. NFV reference points can serve as standard measurement points.

    - **Estimator** - agreed method for measuring and computing the value of a key quality indicator. Often standards such as [i.5] define estimators.

5) **Other Elements** - beyond the scope of this annex.

Figure A.1 illustrates a cloud service customer's primary SLA opportunities:

- **With VNF suppliers** - sample service level specifications are given in Table A.1.

- **With Functional-Component-as-a-Service providers** - sample service level specifications are given in Table A.2.

- **With Management and Orchestration cloud service providers** - sample service level specifications are given in Table A.3.

- **With Service Integrators** - SLAs between cloud service customers and their service integrators will vary based on the specific activities that an integrator was contracted to perform; thus SLAs with service integrators is not considered in this annex.

- **With NFV infrastructure cloud service providers** - sample service level specifications are given in Table A.4.

- **With Cloud Network Service Providers** - SLAs with network service providers are not considered in this annex.

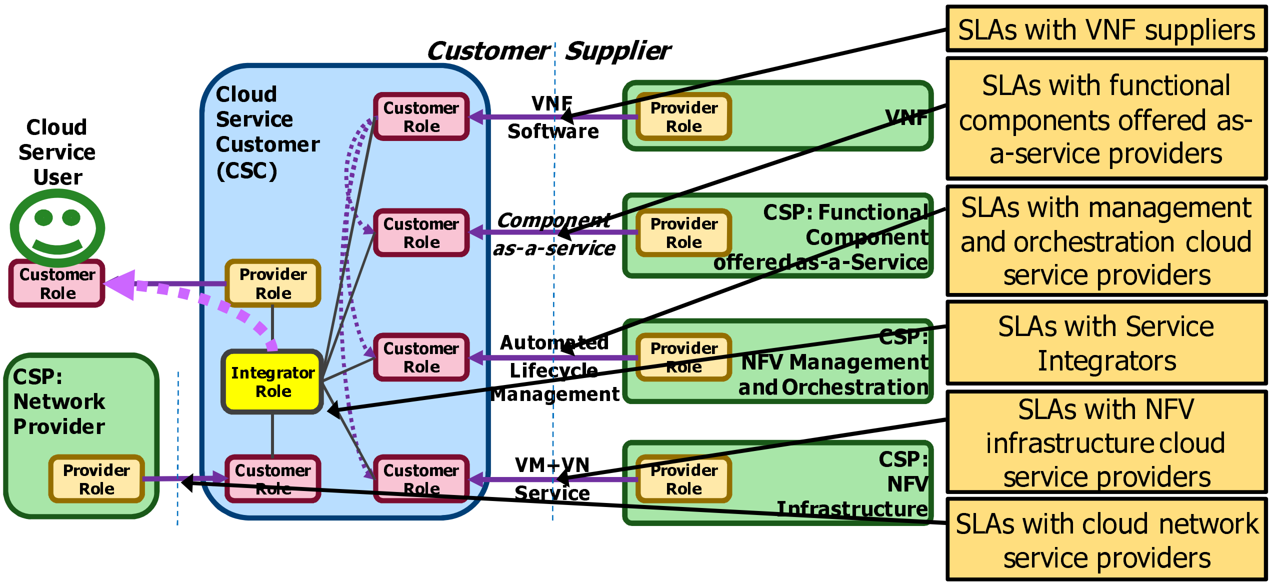

Customer
Supplier
Cloud Service User
Customer Role
Cloud Service Customer (CSC)
Customer Role
Customer Role
Provider Role
Integrator Role
Customer Role
Customer Role
Customer Role
CSP: Network Provider
Provider Role
VNF Software
Component as-a-service
Automated Lifecycle Management
VM+VN Service
Provider Role
VNF
Provider Role
CSP: Functional Component offered as-a-Service
Provider Role
CSP: NFV Management and Orchestration
Provider Role
CSP: NFV Infrastructure
SLAs with VNF suppliers
SLAs with functional components offered as-a-service providers
SLAs with management and orchestration cloud service providers
SLAs with Service Integrators
SLAs with NFV infrastructure cloud service providers
SLAs with cloud network service providers

Figure A.1: Cloud Service Customer's Primary NFV SLAs

Table A.1, Table A.2, Table A.3 and Table A.4 review sample KQIs, measurement points and estimators to include in service level specifications (SLSs) for cloud service customer SLAs for (technical) *service* quality. SLAs for (technical) *support* qualities --- like respond/restore/resolve times --- are not considered in this annex.

Table A.1: Sample Cloud Service Customer SLSs with a VNF Supplier

Key Quality Indicator	Measurement Point	Estimator
Outage Downtime	Vn-Nf	Product-Attributable Service Outage Downtime (SO4) [i.5]
Application-Specific Reliability, Quality and/or Latency KQIs	Vn-Nf	Beyond the scope of this annex.
Defects	-	Number of Problem Reports (NPR) [i.5]

Table A.2: Sample Cloud Service Customer SLSs with a Functional Component-as-a-Service Provider

Key Quality Indicator	Measurement Point	Estimator
Outage Downtime	Vn-Nf (ideally the target VNF's Vn-Nf boundary)	Product-Attributable Service Outage Downtime (SO4) [i.5] OR TcaaS Outage Downtime [i.6]
Service/Transaction Reliability		TcaaS Service Reliability [i.6]
Service/Transaction Latency		TcaaS Service Latency [i.6]
Functional-Component-Specific Reliability, Quality and/or Latency KQIs		Beyond the scope of this annex.
Defects	-	Number of Problem Reports (NPR) [i.5]

Table A.3: Sample Cloud Service Customer SLSs with a Management and Orchestration Cloud Service Provider

Key Quality Indicator	Measurement Point	Estimator
On-Time Completion of Automated Lifecycle Management Actions	Os-Ma-nfvo and Ve-Vnfm-em or Ve-Vnfm-vnf if Cloud Service Provider is accountable for VNFM, OR Or-Vnfm and Vi-Vnfm if Cloud Service Customer is accountable for VNFM	On Time Service Delivery (OTS) [i.5] and [i.8], based on agreed Cloud Service Provider's Promise Times
Service Quality of Automated Lifecycle Management Actions		Service Quality (SQ) [i.5] and [i.8] VM Dead-on-Arrival (DOA) Ratio [i.6] VM Provisioning Latency [i.6] VM Provisioning Reliability [i.6] VN Provisioning Latency [i.6] VN Provisioning Reliability [i.6]
Failure Notification Quality		Failure Notification Timeliness [i.11] Failure Notification Reliability [i.11] Failure Notification Accuracy [i.11]
Placement Policy Compliance	-	VM Placement Policy Compliance [i.6] VN Diversity Compliance [i.6]
Defects	-	Number of Problem Reports (NPR) [i.5] and [i.8]

Table A.4: Sample Cloud Service Customer SLSs with an NFV Infrastructure Cloud Service Provider

Key Quality Indicator	Measurement Point	Estimator
VM Failure Rate	Vn-Nf	VM Premature Release Ratio [i.6]
VM Scheduling Latency		VM Scheduling Latency [i.6]
VM Stall Time		VM Stall [i.6]
Virtual Networking		Packet Delay [i.6] Packet Delay Variation (jitter) [i.6] Packet Loss Ratio [i.6] Network Outage [i.6] Delivered Throughput [i.6]
Infrastructure Provisioning	Vn-Nf and Nf-Vi if NFV Infrastructure Service provider is NOT accountable for VIM, OR Vn-Vnfm and Or-Vi if NFV Infrastructure Cloud Service Provider is accountable for VIM	VM Provisioning Latency [i.6] VM Provisioning Reliability [i.6] VN Provisioning Latency [i.6] VN Provisioning Reliability [i.6]
Defects	-	Number of Problem Reports (NPR) [i.5]

Note that as the functional component as-a-service provider is often also a cloud service customer, the FCaaS provider may have SLAs with both their management and orchestration cloud service provider and their NFV infrastructure cloud service provider(s). Likewise, management and orchestration cloud service providers might have SLAs with NFV infrastructure cloud service providers to support their promise time and quality performance targets.

Annex B (informative): Use Case Scenario

B.0 Introduction

This annex reviews several hypothetical use case scenarios of the quality accountability framework. Scenarios considered:

- B.1 Service Outage Downtime
- B.2 Automated Lifecycle Management Action Failures
- B.3 VM Failure Rate
- B.4 Virtual Network Impairments
- B.5 Virtual Machine Scheduling Latency
- B.6 Virtual Machine Stall Time
- B.7 Functional Components Offered as-a-Service
- B.8 Placement Policy Compliance
- B.9 Resource Promise Violations
- B.10VNF Scaling

B.1 Service Outage Downtime

As explained in clause 7, service impact outage (SO) measurements from [i.5] are used to objectively and quantitatively measure ***outages of end-user service***. Measurement SO2 is defined by [i.5] to measure "*service impact all causes outage downtime per normalization unit per year*." Figure B.1 visualizes the contributors to SO2 for the hypothetical voice mail example of Figure 6 from clause 4.9. All causes user service impact outage downtime (SO2) presented by the cloud service customer offering our sample voice mail service to the cloud service user is logically the sum of the following outage downtimes:

1) **Product attributable outage downtime to the voice mail VNF** (SO4 to the VNF supplier), such as due to critical software failures that produced service impact outage events.

2) **Product attributable outage downtime to the Database-as-a-Service** (SO4 to the DBaaS cloud service provider), such as database downtime that impacts service of voice mail cloud service users.

3) **Outage downtime due to management and orchestration failures** (SO4 to the Management and Orchestration cloud service provider), such as if the management and orchestration service provider fails to continuously enforce the application's anti-affinity rules so a single infrastructure failure event overwhelms the application's no-single-point-of-failure high availability mechanisms to produce user service downtime.

4) **Outage downtime due to infrastructure failures** (SO4 to the NFV infrastructure cloud service provider), such as if a fire in the cloud data centre prompts the infrastructure provider to trigger an emergency power off (EPO) which produces a multi-point failure event that overwhelms the application's high availability mechanism to produce user service downtime

5) Cloud service **customer attributable outage downtime**. [i.5] defines ***customer attributable outage*** as "*An outage that is primarily attributable to the customer's equipment or support activities triggered by:*

   a) customer procedural errors;

   b) office environment, for example power, grounding, temperature, humidity, or security problems; or

   c) one or more of the above.

Outages are also considered customer attributable if the customer refuses or neglects to provide access to the necessary information for the organization to conduct root cause determination."

For example, if the cloud service customer's operational policies maintain insufficient online spare capacity to cover unforecast surges in user demand within the elastic growth lead time period promised by their suppliers, then the user service impact is customer attributable outage downtime.

6) **External attributable outage downtime**. [i.5] defines **external attributable outage** as "*Outages caused by natural disasters such as tornadoes or floods, and outages caused by third parties not associated with the customer or the organization such as commercial power failures, third-party contractors not working on behalf of the organization or customer*". For example, if a natural disaster destroyed the infrastructure service provider's data centre hosting a/the voice mail VNF, then the user service impact might be classified as external attributable outage downtime. External-attributable outages do not appear in the SO measurements, although parties reporting the data are expected to be retain those measurements, if reported to them, for internal use.

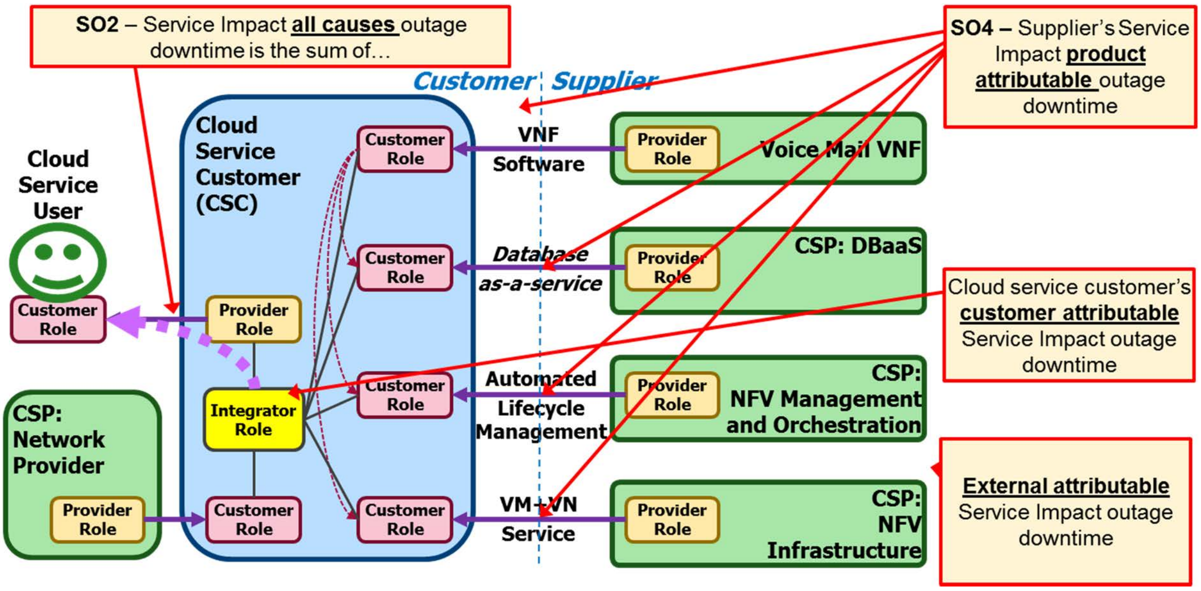

SO2 – Service Impact all causes outage downtime is the sum of…
Customer
Supplier
SO4 – Supplier's Service Impact product attributable outage downtime
Cloud Service User
Customer Role
Cloud Service Customer (CSC)
Customer Role
VNF Software
Provider Role
Voice Mail VNF
Customer Role
Database as-a-service
Provider Role
CSP: DBaaS
Cloud service customer's customer attributable Service Impact outage downtime
Provider Role
Integrator Role
Customer Role
Automated Lifecycle Management
Provider Role
CSP: NFV Management and Orchestration
CSP: Network Provider
Provider Role
Customer Role
Customer Role
VM+VN Service
Provider Role
CSP: NFV Infrastructure
External attributable Service Impact outage downtime

Figure B.1: Service Outage Downtime Example

NOTE: The quality accountability framework does not require any parties to be TL 9000 certified or for any parties to report TL 9000 compliant measurement data. Rather, the quality accountability framework clarifies accountability for outage downtime because rapidly identifying the accountable party accelerates root cause analysis, service restoral and corrective actions to drive continuous quality improvement.

B.2 Automated Lifecycle Management Action Failures

Traditional, manually executed lifecycle management activities like [i.5] product category 7.1.1 "**Installation**" activities (covers new equipment installation, expansion installation, upgrade installation and equipment removal) are vulnerable to human mistakes called **procedural errors**. NFV management and orchestration automates lifecycle management actions like instantiate VNF, upgrade VNF software, scale VNF and heal VNF, but lifecycle management errors are still possible which can cause those actions to fail. Best practice is for cloud service customers to assure clear accountability for avoiding all classes of lifecycle management errors to both minimize the risk of an error event escalating into a user service impacting incident as well as to rapidly identify the accountable party so that root cause analysis and corrective actions can be completed promptly to drive continuous quality improvement.

The standard definition of **procedural error** from [i.5] is a solid foundation when considering (traditional) lifecycle management failures:

An error that is the direct result of human intervention or error. Contributing factors can include but are not limited to:

a) deviations from accepted practices or documentation;

b) inadequate training;

c) unclear, incorrect, or out-of-date documentation;

d) inadequate or unclear displays, messages, or signals;

e) inadequate or unclear hardware labeling;

f) miscommunication;

g) non-standard configurations;

h) insufficient supervision or control; or

i) user characteristics such as mental attention, physical health, physical fatigue, mental health, and substance abuse.

Examples of a Procedural Error include but are not limited to:

a) removing the wrong fuse or circuit pack;

b) not taking proper precautions to protect equipment, such as shorting out power, not wearing ESD strap, etc.;

c) unauthorized work;

d) not following Methods of Procedures (MOPs);

e) not following the steps of the documentation;

f) using the wrong documentation;

g) using incorrect or outdated documentation;

h) insufficient documentation;

i) translation errors;

j) user panic response to problems;

k) entering incorrect commands;

l) entering a command without understanding the impact; or

m) inappropriate response to a Network Element alarm.

A parallel definition of ***lifecycle management error*** is as:

an error that is the direct result of policy, management, or orchestration. Contributing factors can include but are not limited to:

a) deviations from accepted practices or documentation;

b) faulty or out of date: automation scripts, policies; service, VNF or resource descriptors, etc.;

c) inadequate, insufficient or stale FCAPS input data;

d) non-standard configurations;

e) insufficient supervision or control;

f) faulty execution of policy by a management or orchestration element;

g) tardy execution of lifecycle management action;

h) risky operational policies.

Examples of lifecycle management errors include but are not limited to:

1) Maintaining insufficient spare online capacity to serve lead time demand, random variations and unforecast surges in demand, and mitigate user service impact of failure events.

2) Failing to diligently monitor alarms and correct unsuccessful VNF repair actions which leave impacted VNF simplex exposed.

3) Failing to continuously enforce anti-affinity placement rules for VNFCs can lead to both primary and protecting VNFC instances appearing in a single NFV infrastructure failure group.

4) Inadequate, insufficient or stale performance information which produce faulty elastic capacity management decisions.

Cloud service customers have to implement processes, policies, architectures, mechanisms and make supplier and service provider selections to minimize or prevent end user service impacts caused by lifecycle management errors. Part of that assurance is clarifying responsibilities of the VNF suppliers, service integrators, cloud service providers and the cloud service customer to assure responsibilities and accountabilities properly interlock to minimize the risk that any automated lifecycle management error escapes, activates and cascades into a service impact outage event.

B.3 VM Failure Rate

High availability VNFs are designed to mitigate single point failure events without accruing chargeable service outage downtime. However, an infrastructure failure event that impacts a single VNFC might produce a sub-critical (i.e. non-outage) user visible service impact to transactions that were queued or in-flight at the instant of failure; for example, impacted transactions might have to be retried (adding service latency) and RTP packets of bearer traffic queued or in-flight in the impacted VNFC might be lost (forcing client devices to engage lost packet compensation algorithms). VNF supplier is accountable for the user service impact per VM failure event, while the NFV infrastructure service provider is accountable for the rate of VM failure events (called premature VM release rate in [i.6]). If the VM failure rate reaches epidemic proportions, then special arrangements between the cloud service customer and the NFV infrastructure service provider may be appropriate.

B.4 Virtual Network Impairments

NFV infrastructure service providers, possibly in conjunction with CSP:network providers, are accountable for transporting packets between VNFCs within a single VNF instance, as well as between a target VNF and other VNFs, PNFs, functional components offered as-a-Service and to cloud service users' devices. VNFs will implement packet timeout and retransmission mechanisms, de-jitter buffers, automatic failover and other mechanisms to mitigate the user service impact of virtual network impairments; however, the frequency with which those mechanisms engage is determined by the actual virtual networking service quality delivered by the infrastructure service provider and applicable CSP: network providers. For example, a virtual network transient incident that persists for hundreds of milliseconds might cause a highly available bearer plane VNF to failover service to a redundant VNFC. As the root cause of the service failover is the virtual network transient incident, the aggregate service impact of that virtual network transient incident and subsequent failover is attributable to the infrastructure service provider (or applicable CSP:network provider).

B.5 Virtual Machine Scheduling Latency

VM Scheduling Latency is defined in [i.6] as "*the absolute value of the difference between when a guest operating system event should have executed and when the event actually executed*". Many real time and bearer plane VNFs rely on regular (e.g. 1 millisecond) timer interrupts to drive isochronous processing to assure that bearer traffic is efficiently processed without introducing jitter or excess delay into the flow. Virtualisation software, along with other VNF tenants who might be sharing physical hardware, introduce risks that timer interrupts will not be delivered to the target VNF software when requested, thereby introducing excess delay which appears to the end user as jitter in the stream of received data.

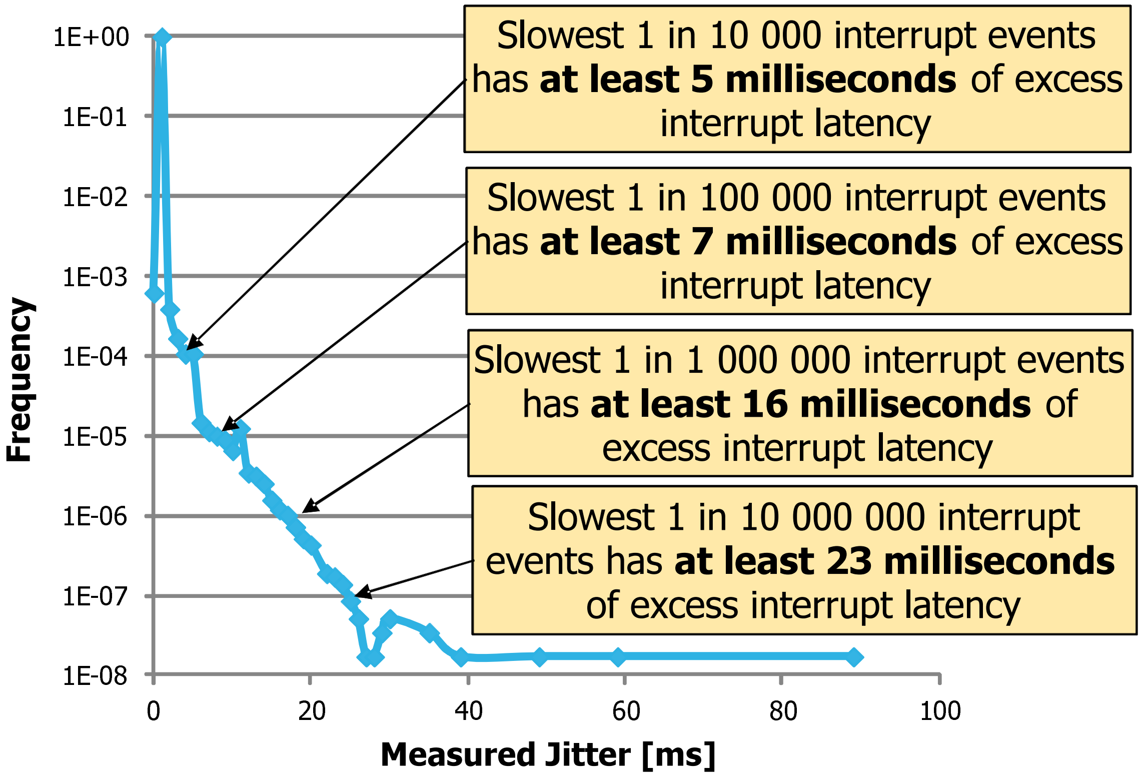


Figure B.2: Sample 1 Millisecond Timer Interrupt Scheduling Latency

Figure B.2 shows the distribution of actual activations of 1 millisecond timer events for a VNF running on a commercial hypervisor with default configuration. The slowest 1 in 10 000 interrupt (once every 10 seconds) has at least 5 milliseconds of excess latency; the slowest 1 in 100 000 interrupts (once every 2 minutes) has at least 7 milliseconds of excess latency; the slowest 1 in 1 000 000 interrupts (once every 17 minutes) has at least 16 milliseconds of excess latency; the slowest 1 in 10 000 000 interrupts (once every 3 hours) has at least 23 milliseconds of excess latency. Different hypervisors, hypervisor configurations, operational (e.g. multi-tenancy, placement) policies and other factors may produce more or less interrupt scheduling latency for any particular VNF.

As timer interrupt scheduling latency is entirely controlled by the infrastructure service provider there is literally nothing a VNF can do to mitigate scheduling latency introduced by the infrastructure, because the VNF software simply cannot do anything when it is not being executed by the infrastructure. Thus, the cloud service customer works with the management and orchestration cloud service provider to assure that sensitive VNFs are placed onto infrastructure that is configured to assure that timer interrupts are delivered to their VNFs with acceptable scheduling latency.

B.6 Virtual Machine Stall Time

The VM Stall metric is defined in [i.6]. Elements with real time performance expectations are particularly sensitive to VM stall events because while the VM is stalled, packets typically accumulate in buffers rather than being processed promptly. If the stall event persists for more than a few milliseconds, such as during a live VM migration event, then impacted client applications may retry or even abandon requests, be forced to engage lost packet compensation mechanisms or take other mitigating actions on impacted service requests or data flows.

To make it feasible and likely that all processing by the cloud service customer's VNFs will be timely enough to assure acceptable quality of experience by cloud service users, cloud service customers may stipulate a maximum acceptable VM stall time for VNFCs that are highly sensitive to VM stall events (e.g. no VM stall event > ***x*** milliseconds). The management and orchestration cloud service provider, in coordination with the infrastructure cloud service provider, could place those VNFCs onto infrastructure elements --- especially hypervisors --- that were engineered, configured and operated to assure that VM stall events never exceed the cloud service customer's stipulated value.

B.7 Functional Components Offered as-a-Service

Cloud service provider: functional component offer the service of common functional components like database and load balancers that can be integrated into service chains to shorten service creation times and otherwise benefit a cloud service customer. [i.6] defines three primary service quality metrics for functional components offered as-a-Service (called technology components in [i.6]):

- **Functional component as-a-service (TcaaS) reliability** for as the reliability of specific operations offered by the component, like the database update defects per million (DPM) rate for a database-as-a-service offering.
- **Functional component as-a-service (TcaaS) latency** for specific operations offered by the component, like transaction latency of database update operations for a database-as-a-service offering.
- **Functional component as-a-service (TcaaS) outage downtime** for the service enjoyed by the cloud service customer, such as service outage downtime for database operations for a database-as-a-service offering.

VNFs actually consume functional components offered as-a-Service across the Vn-Nf reference point of the VNF's applicable VNFC instances, as shown in Figure B.3 as the dashed vertical line adjacent to target VNF 1 and target VNF 2. The VNFs implementing the target functional component offered as-a-service operate in the same cloud data centre as target VNF 1, so NFV infrastructure service provider 1 has accountability for virtual network connectivity between target VNF1 and the target functional component offered as a service. Target VNF 2 uses the same target functional component offered as-a-service, but VNF 2 resides in a different cloud data centre operated by NFV infrastructure service provider 2, and a CSP: network provider is accountable for network connectivity between NFVI service provider 1 and NFVI service provider 2.

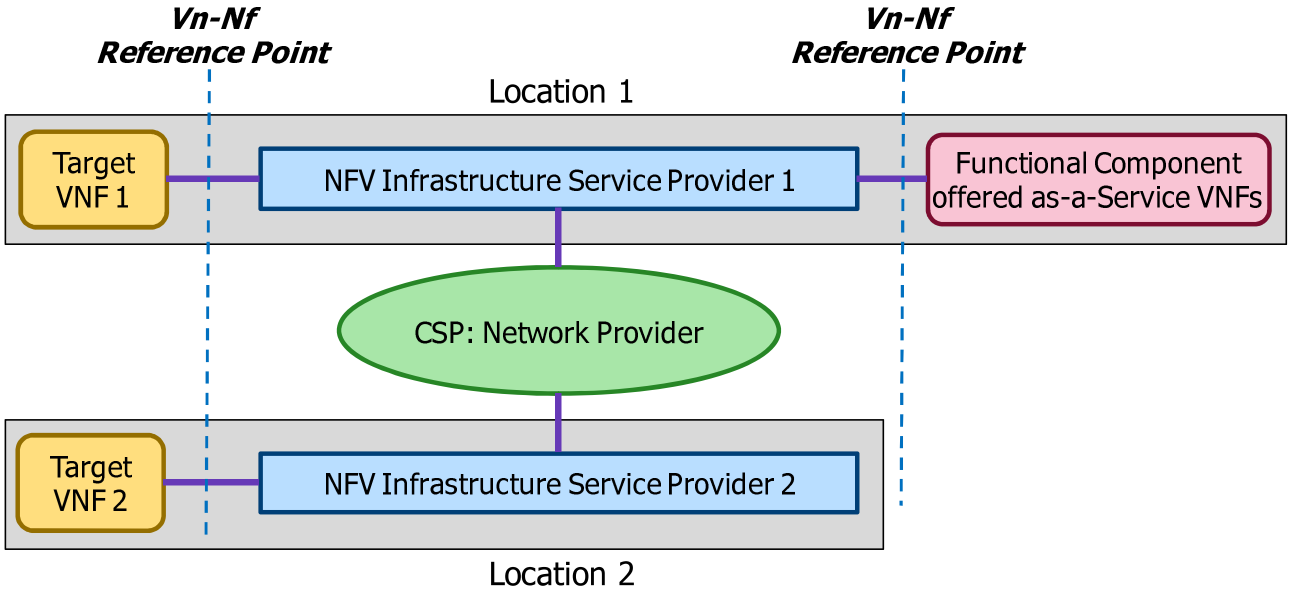

Vn-Nf
Reference Point
Vn-Nf
Reference Point
Location 1
Target VNF 1
NFV Infrastructure Service Provider 1
Functional Component offered as-a-Service VNFs
CSP: Network Provider
Target VNF 2
NFV Infrastructure Service Provider 2
Location 2

Figure B.3: Sample Functional Component as-a-Service Accountability Framework

Virtual connectivity between collocated target VNFs and functional components offered as a service is vulnerable to the virtual network impairments in [i.6], such as packet loss, packet latency and jitter; those virtual network impairments should be attributed to the NFVI provider serving that location. Non-collocated arrangements insert a second NFVI provider and at least one CSP:network provider who can introduce virtual network impairments into the critical path. The Management and Orchestration service provider's VNF placement decision can materially impact the aggregate virtual network impairment vulnerability of a service chain that uses technology components offered as a service, thus those placement decisions need to consider the service quality promises of applicable NFVI providers and CSP:network providers to assure that the cloud service provider's quality expectations across the target VNF's Vn-Nf reference point can be met with proposed VNF placement and functional component as-a-service configuration.

B.8 Placement Policy Compliance

The management and orchestration service provider has primary accountability for placing VNF components instances onto virtual infrastructure in compliance with the cloud service customer's applicable anti-affinity rules, descriptors and policies (as well as complying with applicable cloud service provider policies and constraints). Beyond the initial placement decision, the management and orchestration service provider has primary accountability for assuring that those placement policies are continuously enforced during operational, scaling, healing and other phases of VNF and network service lifecycles. By returning success to cloud service customers when executing an automated lifecycle management action, the management and orchestration service provider takes accountability for both the correctness of that placement decision as well as for continuous enforcement of those placement policies. For instance, if a management and orchestration service provider fails to continuously enforce anti-affinity rules across time and a series of scaling and healing lifecycle management actions ultimately place both primary and protecting VNFCs onto a single infrastructure element which subsequently fails and overwhelms the VNF's high availability mechanisms (because the single infrastructure element failure creates a correlated, multipoint failure for the VNF), then the management and orchestration service provider is accountable for the user service impact. In some cases it may not be possible for a management and orchestration service provider to make placement decisions that fully conform to all stipulated anti-affinity rules, descriptors and policies, such as if compliant resource capacity is not available. If the management and orchestration service provider notifies the cloud service customer that it cannot comply with one or more placement anti-affinity rules, descriptors or policies, then the management and orchestration service provider is not accountable for continuously enforcing that specific rule.

B.9 Resource Promise Violations

Infrastructure service providers, like airlines and hotels, may oversubscribe their resources. If an airline failed to permit a ticketed passenger to take their seat because the airline had oversold a flight, then the airline is accountable for the passenger's inconvenience. Likewise, if the infrastructure service provider is unable or unwilling to promptly deliver the promised resource throughput (i.e. the capacity rating of the successfully allocated resource), then user service impact is attributable to the infrastructure service provider.

B.10 VNF Scaling

Per [i.9], the *Scale VNF* operation is offered both by the VNFM to the NFVO across the Or-Vnfm reference point and by the NFVO for the OSS across the Os-Ma-nfvo reference point, as shown in Figure B.4.

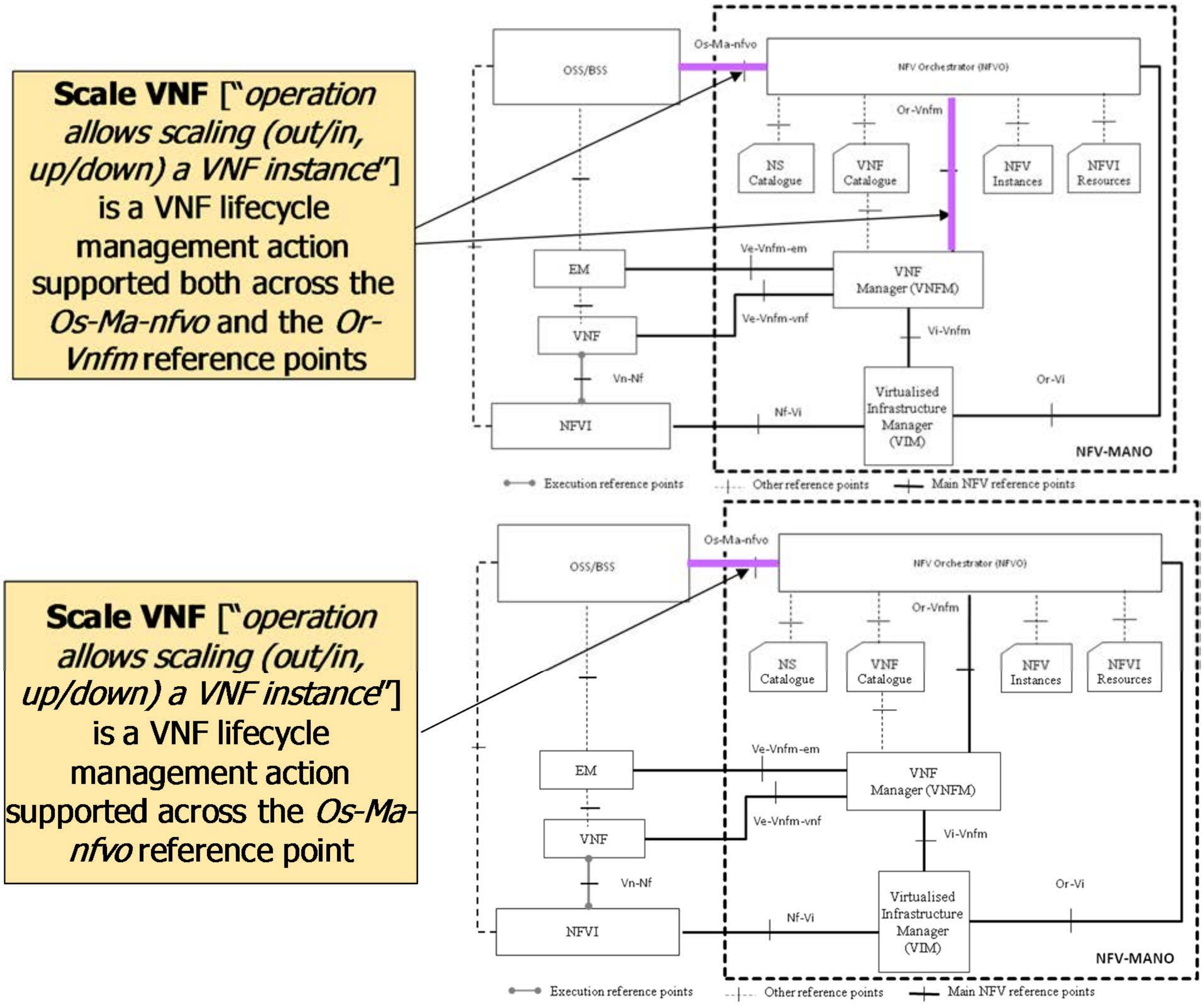

Scale VNF ["operation allows scaling (out/in, up/down) a VNF instance"] is a VNF lifecycle management action supported both across the Os-Ma-nfvo and the Or-Vnfm reference points
OSS/BSS
Os-Ma-nfvo
NFV Orchestrator (NFVO)
Or-Vnfm
NS Catalogue
VNF Catalogue
NFV Instances
NFVI Resources
EM
Ve-Vnfm-em
VNF Manager (VNFM)
VNF
Ve-Vnfm-vnf
Vi-Vnfm
Vn-Nf
Or-Vi
Virtualised Infrastructure Manager (VIM)
NFVI
Nf-Vi
NFV-MANO
Execution reference points
Other reference points
Main NFV reference points
Scale VNF ["operation allows scaling (out/in, up/down) a VNF instance"] is a VNF lifecycle management action supported across the Os-Ma-nfvo reference point
OSS/BSS
Os-Ma-nfvo
NFV Orchestrator (NFVO)
Or-Vnfm
NS Catalogue
VNF Catalogue
NFV Instances
NFVI Resources
EM
Ve-Vnfm-em
VNF Manager (VNFM)
VNF
Ve-Vnfm-vnf
Vi-Vnfm
Vn-Nf
Or-Vi
Virtualised Infrastructure Manager (VIM)
NFVI
Nf-Vi
NFV-MANO
Execution reference points
Other reference points
Main NFV reference points

Figure B.4: A VNF Scaling Measurement Point

Objective and quantitative measurement of automated lifecycle management actions, such as VNF scaling, can be made using [i.8] at specific measurement points, such as the Os-Ma-nfvo NFV reference point, as follows:

- **Supplier promise time** - what is the cloud service provider's delivery commitment to the customer for VNF scaling actions across the *Os-Ma-nfvo* reference point, such as "*30 minutes or less*".

- **On-time delivery percentage** - what portion of VNF scaling actions complete within the cloud service provider's (supplier) promised time, such as "*95 % of VNF scaling requests will be fulfilled within the promised time*".

- **Service quality** - what portion of VNF scaling actions are found by the cloud service customer to have completed successfully, such as "*99 % of VNF scale requests will be completed correctly*".

Just as traditional retailers have to consider their suppliers' lead times and order fulfilment qualities when determining when to restock their physical inventories, cloud service customers will have to consider their cloud service provider's VNF scaling promise time, on-time delivery percentage and service quality, as well as cyclical and random patterns of application demand and other factors, when deciding exactly when to request VNF scaling actions. Traditional retailers often maintain a safety stock of inventory to cover perhaps two lead time intervals, and cloud service customers are likely to maintain sufficient spare (a.k.a. safety) online application capacity to cover forecast and random variations in demand, as well as failures, for several supplier promise time intervals. Thus, a cloud service customer can potentially maintain a smaller margin of spare online capacity to assure a particular service level when served with a high quality 15 minute VNF scaling promise time than they need to maintain if served by a 2 hour VNF scaling promise time.

Annex C (informative): Overview of TMForum and QuEST Forum Roles

Figure C.1 visualizes the key mapping between TMForum [i.3] SLA roles and [i.5] roles: a TL 9000 "supplier" (or TMForum "service provider") offer a "product" (which could be a service) that is defined by a [i.5] product category to a TL 9000 (or TMForum) "customer".

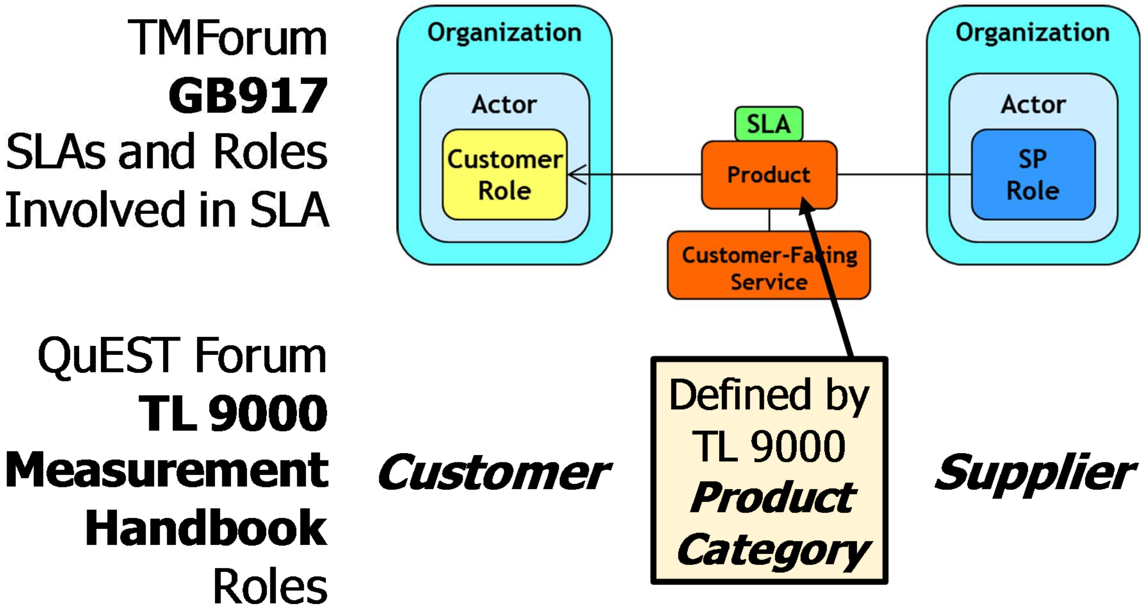


Figure C.1: Overview of TMForum and QuEST Forum Roles

Annex D (informative): Administrative Domains and Accountable Parties

[i.9] introduces administrative domains as an architectural concept:

- **Administrative Domain** - collection of systems and networks operated by a single organization or administrative Authority

NOTE: The components which make up the domain are assumed to interoperate with a significant degree of mutual trust among them based on a stable trust relationship, while a transient, specific trust relationship can be established for interoperating with components in other domains [i.9]. [i.9], clause 4.7 "**Administrative Domains**" goes on to say "...the following administrative types of domains are identified:

  - Infrastructure Domain.
  - Tenant Domain."

- **Infrastructure Domain** - administrative domain that provides virtualised infrastructure resources such as compute, network, and storage or a composition of those resources via a service abstraction to another Administrative Domain, and is responsible for the management and orchestration of those resources [i.9].
- **Tenant Domain** - domain that provides VNFs, and combinations of VNFs into Network Services, and is responsible for their management and orchestration, including their functional configuration and maintenance at application level [i.10].

The Quality Accountability Framework focuses on the accountable **parties** (e.g. cloud service customer organizations, NFV management, orchestration and infrastructure service provider organizations, and VNF supplier organizations) who act as either a customer or a supplier/service provider for a particular product (which could be a service), as described in a**nnex C - Overview of TMForum and QuEST Forum Roles**, and have responsibilities with respect to their counterparties (discussed in clause **5 Responsibilities by Role** and clause **6 Responsibilities by Key Cloud Characteristics**). Supplier/service provider roles may be held accountable via service level agreement or other arrangement for delivering their product/service to agreed quality expectations.

Cloud Service Customers and NFV management and orchestration service providers operate within the tenant domain and NFV infrastructure service providers operate within the infrastructure domain. However [i.9] does not explicitly consider either VNF suppliers, service integrators, or functional-component-as-a-service providers so there is no defined mapping of those roles to administrative domains.

Annex E (informative): Authors & contributors

The following people have contributed to this specification:

Rapporteur:
Dr. Julien Maisonneuve, Alcatel-Lucent

Author:
Mr. Eric Bauer, Alcatel-Lucent

Annex F (informative): Bibliography

Reliability and Availability of Cloud Computing by Eric Bauer and Randee Adams, Wiley-IEEE Press, August 14, 2012.

Service Quality of Cloud-Based Applications by Eric Bauer and Randee Adams, Wiley-IEEE Press, December 31, 2013.

History

Document history		
V1.1.1	January 2016	Publication