INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2017-2020

SG13-TD239/WP2

STUDY GROUP 13

Original: English

Question(s): 19/13 Geneva, 18 April 2018

TD

Source: Associate rapporteur

Title: Living list for Q19/13

Purpose: Information

Contact: Emil Kowalczyk
Orange Polska
Poland
Tel: +48 502 397 809
Email: Emil.Kowalczyk@orange.com

Contact: Ying Cheng
China Unicom
P.R.China
Tel: +86-10-66259394
Fax: +86-10-66259154
Email: chengying10@chinaunicom.cn

Keywords: Output; Living list; Q19/13

Abstract: This document is the output of living list for Q19/13. It includes the discussion results during the Q.19/13 meeting held on 9-18 April 2018.

This is the revised living list based on the meeting results of Q19/13 held in Geneva, 9 – 18 April, 2018.

During ITU-T SG13 Q19 meeting, the following contribution was discussed, and agreed to be included in the living list of Q19.

Doc Num.	Sources	Title	Question
[C-86]	India	Proposal of new work item on "Predictive Fault and performance management to ensure carrier grade reliability and availability of virtual network services on multiple clouds"	Q19/13

In addition, the material of "Living list #2: Framework of big data preservation" were removed due to acceptance contribution **[C-102],** material of "Living list #3: Cloud service evaluation index" were removed due to acceptance contribution **[C-14]**.

Deleted: Note - Insertion of an issue into the Living List is generally based on contributions and requires a general agreement that the issue is important for further consideration. ¶
Proposal should include texts conforming to the Recommendation structure and provide for enhancements and/or modifications of the relevant parts of the Recommendation. ¶
An issue is deleted from the Living List if no contributions addressing the issue have been provided in a long period and there is a general consensus for its removal. When an item is added to the living list, its status is U by default. ¶
Transition from U to P may happen at the next meeting if there is a consensus on the solution proposed in the form of modifications to the current text of the Recommendation and if no contradicting contribution is provided. Transition from P to F may happen at the next meeting if no contribution contradicts the provisionally agreed text and there is consensus.¶
When contribution (s) are provided contradicting the existing text with status "P" and no consensus is achieved on the contribution, the status of the existing text is unchanged. Transition from P to U happens only if consensus is achieved on the contradicting contribution.¶
Frozen texts are inserted in the updated version of the Recommendation if there is consensus.¶
This is the Q19/13 general living list (including for new work item proposals).

Deleted: This document is based on the following documents. ¶
Various ...

<Living List structure and procedures>

The following Living List structure and procedures are intended to progress the work under Q19/13.

1. Structure

A. List of Items

- Title of item

B. Description of each item

- Title
- Description of the problem and possible solutions
- List of documents addressing the issue
- Intermediate agreements

2. Status of proposals

Status of proposals

U – Under study

P – Provisionally agreed

F – Frozen

3. Guidelines

- Insertion of an issue into the Living List is generally based on contributions and requires a general agreement that the issue is important for further consideration.
- Proposal should include texts conforming to the Recommendation structure and provide for enhancements and/or modifications of the relevant parts of the Recommendation.
- An issue is deleted from the Living List if no contributions addressing the issue have been provided in a long period and there is a general consensus for its removal.
- When an item is added to the living list, its status is U by default.
- Transition from U to P may happen at the next meeting if there is a consensus on the solution proposed in the form of modifications to the current text of the Recommendation and if no contradicting contribution is provided.
- Transition from P to F may happen at the next meeting if no contribution contradicts the provisionally agreed text and there is consensus.
- When contribution (s) are provided contradicting the existing text with status “P” and no consensus is achieved on the contribution, the status of the existing text is unchanged. Transition from P to U happens only if consensus is achieved on the contradicting contribution.
- Frozen texts are inserted in the updated version of the Recommendation if there is consensus.

4. Operational rules

- All proposed modifications to the Recommendation should be made available to the ITU-T meetings in a PC compatible electronic version.

Q19/13 living lists

No.	Title of Living Lists	Status
1	Trusted Cloud Scenarios	Under Study (May 2015) Retained (June 2016) Reviewed and noted as useful and inspirited material for future trusted cloud framework and related recommendations e.g. functional architecture of trusted cloud, (February 2017)
2	Proposed content for clause 8 and 9 of Y.CCICTM	Under Study (November 2017) This material provides functionalities for managing isolation and security mechanism, and requirements for inter-cloud trust management. But currently there are no use cases to support these requirements. Use cases should be provided in the future to move this content to the draft Y.CCICTM.
3	Proposed new WI "Predictive Fault and performance management to ensure carrier grade reliability and availability of virtual network services on multiple clouds"	Under Study (April 2018) This material provides the proposal for new work item "Predictive Fault and performance management to ensure carrier grade reliability and availability of virtual network services on multiple clouds". Clarification for scope and main focus of this proposed new work item are needed.

Deleted: 2

Deleted: 4

Living list #1: Trusted Cloud Scenarios

This document represents a set of cloud security use cases intended to inform the collaborative work on cloud security in Study Group 13 and Study Group 17.

1 The Hospital Patient

Adam visits the local hospital for investigation of a potentially serious medical problem. The hospital uses cloud computing for the storage and processing of medical records. Medical staff at the hospital are able to enter, examine, and modify medical records from a variety of fixed and mobile devices including specialist terminals (e.g. X-ray suites), PCs, tablets, and smartphones. Staff, patients and visitors may also have their own personal devices.

1.1 Certification

The hospital is governed by local regulations on the strict confidentiality of medical information. These regulations are different from those in other countries. The cloud service provider is certified under the relevant standards and local regulations to handle this information correctly.

1.2 Confidentiality

Adam needs reassurance that his medical records will not be made available to anyone without his explicit authorisation, and for purposes to which he has agreed. He is particularly concerned that his name and identity should not be associated with his visit, nor with any medical terms relating to his condition.

All of the hospital devices are protected with encrypted storage, and their medical software runs in a secure sandbox that prevents data being shared with any other apps on the device, and ensures that any data is wiped if the device is lost or stolen. Any devices that do not have a suitable sandbox are limited to accessing medical information via a protected web page only, with no local cache or storage on the device.

1.3 Indirect Storage

The cloud service provider employs another cloud service (from another CSP) for backup and archiving of the patient data. Although this data is stored in an encrypted form, to which the storage CSP has no keys, local law requires them to identify the stored data as confidential patient data, and to be certified for proper handling of it.

2 Enterprise Customer

Brioche Investments, a specialist French finance house, adopts a hybrid cloud model for their global IT system. They use a public cloud for much of their “regular” business, such as employee email and documents, with their own secure datacentre outside Paris for critical information such as audit records, customer accounts information, and legal documents.

2.1 Business Continuity

Brioche maintain a constantly updated backup of their private cloud data and audit trails to the public cloud. This backup is encrypted, with Brioche retaining the encryption keys, such that the public cloud is unable to examine their backups. In the event of a failure of their own datacentre, Brioche have the option of either bringing their backup home, or of creating a virtual datacentre in the cloud.

2.2 Regulatory Compliance

Being an EU company, Brioche is required to adhere to the data protection regulations of France and the EU. As such, Brioche is only able to use cloud services that are either based in the EU, or that meet the requirements for Safe Harbour of EU data.

2.3 CSP Governance

The board of Brioche are concerned that their CSP is well organised, has transparent and clear lines of authority and policy making, and is able to fully understand and implement the requirements placed upon them.

Personally Identifiable Information

Brioche requires their cloud service provider to be certified for adherence to international standards for handling and control of PII.

Transparency of Purpose

Brioche are considering moving their in-house CRM system to a public cloud offering. They want to compare various services, however they are very concerned that the valuable client data they would enter into such a system is not exploited for purposes other than their own applications, and cannot be mined by either the service provider or any other organisation. They therefore require clear and binding statements on exactly how their data will be handled and that cannot be changed by the service provider without Brioche's explicit consent.

3 Business Traveller

George is an independent lawyer who represents people who have disputes with their employers or their local government, including cases of whistleblowing over corruption. As these people are often unable to travel themselves, he usually visits them wherever they are, by car, train, or aircraft. He also has to visit the other parties, wherever they may be.

George needs access to all of his case information, and to his legal databases, from wherever he is at the time. He uses a secure cloud service to store and manage his various documents.

Secure Access

Since George is often connecting with whatever network is available, he needs secure connections to his cloud service so that his communications cannot be intercepted. For this reason, he uses a strongly encrypted virtual connection from his tablet, phone, or PC to his cloud service provider.

Secure Device

George is always concerned that a corrupt official could seize his device and attempt to access George's records. He therefore uses a service that synchronises all of his documents securely to the cloud, keeping a local offline copy only in a securely encrypted form which can be rendered unusable if attempts are made to hack into it.

Multi-factor authentication

Because of the importance of trust, George is very concerned about the risk of his account being hijacked. He insists that his service provider only accept connections to his account that have been authenticated by multiple secure means.

4 Local Government

Barchester District Council has decided to close down their outdated and expensive IT installation and move to a hybrid cloud system run by the larger neighbouring Wyvern County Council. Wyvern uses a mixture of in-house servers, together with public cloud resources and network services provided by Wessex Telecom. Wyvern already have a number of other local governments using their platform.

Certification

Barchester and Wyvern both have to meet stringent legal requirements for their IT systems, especially as they contain very sensitive data such as social services records (including child protection files), and employee records for thousands of public servants. Barchester does not have the resources or expertise to audit Wyvern's cloud system. They therefore need to see independent certification of the security of Wyvern's system, and need access to audit reports and SLA monitoring from Wyvern. Barchester's Council's primary concern is to protect themselves from any legal exposure arising from any security failure or breach at Wyvern.

Secure Access

Barchester has a number of councillors who have a deep distrust of the Internet, both in terms of reliability and security. Barchester therefore decides they need a dedicated private connection between their council offices and the Wyvern datacentre. This link is provided as a private connection by Wessex Telecom, and does not go over the public Internet. This link is also encrypted at both ends to prevent any attempted interception by Wessex Telecom or their employees.

Legacy Interoperability

Barchester uses a wide variety of legacy systems across their various departments. It will not be possible to replace all of them before the move to the cloud, so it will be necessary to support these legacy systems and their security mechanisms during the cloud transition phase.

5 Corporate Device User

Adam works for the Bank of Sodor. They provide him with a cellphone and a tablet, both of which allow him to connect to the private cloud services operated by his employer.

Secured devices

The Bank of Sodor requires that all devices used to access the bank's internal services are secured by multiple levels of protection.

- Firstly, they require every device to be tested and approved by their IT security department.

- Secondly, the storage of every device is fully encrypted so that it cannot be read if stolen, even if disassembled. Repeated failures to sign in correctly make the device unusable.
- Thirdly, the bank is able to remotely lock or destroy any such device, or to render it completely unusable even when the password(s) are known to the person in possession of the device.
- Fourthly, the bank can use a cloud service to obtain a recent location of each device should the need arise.

Secured connections

The Bank requires that all communications from bank-owned devices are routed through a permanent VPN, such that all communications whether by the user or by an app can be screened and verified. Connections via WiFi or cellular data, no matter which website or cloud they are directed to, must all go through the bank's firewalls. The VPN is strongly encrypted.

Restricted Platform

The Bank requires control over which apps can be installed to devices, and how they are connected to cloud services. Adam has access to a variety of apps from public application marketplaces, provided they are approved by the bank. He also has access to set of corporate apps made available by the bank, most of which connect to the bank's private cloud services.

6 Government Agency - Data Location

The government of Ruritania (a small state within the EFTA) moves much of their data processing to public cloud computing. They decide to use a combination of SaaS, PaaS and IaaS services from multiple cloud service providers. All of these services store and share information using the cloud storage capabilities of cloud services.

Cloud Storage Policies

The government of Ruritania has reviewed their data storage regulations, identified areas where it was based on outdated assumptions of in-house storage, and developed new policies that allow for appropriate use of cloud storage. The policy defines various categories of data. Depending on the category, various rules are to be applied.

1. The data is stored and processed only in Ruritania government computers on government premises
2. The data is only processed and stored within the EFTA area.
3. The data is only processed within the EFTA, but encrypted copies may be stored or backed up globally. Processing outside the EFTA is permitted only for continuity in the event of a major disaster or outage, with the Government's explicit approval
4. The data can be processed or stored anywhere, provided the service provider contracts include the EU model clauses for data protection, and the service provider is certified for ISO 27001 with the 27018 controls.
5. The data can process and stored anywhere, with any provider (for example the contents of the government's Facebook page for tourism).

Government policy makes clear to their officials on how data should be categorised.

Storage Account Creation

The Ruritania Tourism Authority (RTA) creates cloud storage accounts for several different cloud services. Depending on the service, the RTA chooses a cloud service provider who can provide storage that meets or exceeds the requisite data location policies.

As the Data Controller, the RTA is responsible for categorising their data and directing it to the appropriate storage account. The cloud service provider does not want to make these decisions, as they do not want to be regulated as a Data Controller.

Storage Monitoring

The RTA uses facilities provided by the cloud service provider(s) to monitor their storage usage, including the locations where their data is being stored.

7 Cloud Service Migration

Acme Manufacturing has been using cloud services from a cloud service provider called CheapCloud. They have become dissatisfied with the quality of the service they are receiving, and decide to migrate to another cloud service provider "SmartCloud".

The services that CheapCloud have been providing consist of:

- Cloud based email
- Cloud based document storage and editing
- Hosting a number of IaaS virtual machines

One of the reasons to select SmartCloud is that they are running software that is broadly similar to that used by CheapCloud.

Notification of service cancellation

Acme invokes the termination clause of their contract with CheapCloud. CheapCloud is required by the contract to provide Acme with current copies of all data, and then to completely remove the data from their system.CheapCloud are required to provide everything in a form that can be ingested or run on other systems, either in-house at Acme or on another cloud service.

Note: cloud service portability is being studied in ISO/IEC SC38 WG4, which is developing a new standard ISO/IEC 19941 "Information technology – Cloud computing – Interoperability and Portability". Information on this draft standard can be obtained from your ISO National Body. This standard addresses various aspects of cloud portability, including data, application, and virtual machine, together with many of the engineering problems associated with these operations.

Migration of User Accounts

Acme downloads the current list of their employee accounts from CheapCloud. They then need to convert this into a batch submission to create matching accounts at SmartCloud. This is complicated by the need to create new passwords for everyone, however a smart engineer at Acme is able to write a script that automates this to some extent.

Migration of Email

Acme's DNS entries are updated to route incoming email to their new service provider. Incoming email now arrives at the new email accounts.

The existing content of email boxes at CheapCloud has to be downloaded and posted to the matching email boxes at SmartCloud. This causes some concerns, because confidential email will need to be processed in the clear to make this happen. Eventually they create a special team of trusted long-service employees to handle this process, under close scrutiny by the legal department.

Migration of Virtual Machines

It is necessary to shut down all the hosted virtual machines in a known state before they can be copied to the new service.

Due to the size of the VM files, they are copied to physical media and transported by road to Acme and then to the new service provider for loading. This causes a three day service interruption, because it is not possible to keep the VMs running due to lack of synchronisation between the old and new environments.

When the VMs are loaded and started, Acme learns that some of their configuration does not match the new IaaS environment, some network settings such as firewall ports do not match, and it takes several days to get their core line of business applications working correctly in the new environment.

Migration of Documents

Acme experience a number of issues with migrating their stored documents. While both cloud providers use the same document format (ISO ODF) it becomes clear that there are differences in implementation of the web-based document editing, such that some documents do not render correctly on the new system and have to be manually reworked.

Also, it soon becomes clear that change tracking and comments embedded in many of the documents is corrupted. The reason emerges that these are tied to the identity key of the user who made the note or change, and that these keys are different on the new system. Thus, comments and markup are attributed to the wrong person, or lost entirely since the system cannot cope with comments for which the author does not exist.

The legal and HR departments also express concern that their documents should not be seen by other departments. It therefore becomes necessary for each department to allocate staff to handle the migration of their department documents from the old to the new systems.

Fallout

A few weeks after the migration it is discovered that some files were converted incorrectly during the process and are no longer usable. Enquires of CheapCloud are met with the response that under the contract terms they no longer have copies of the lost data. Fortunately, the physical media used to transport the files have not yet been erased or reused, and the files can be recovered from there.

8 Cloud Service Outage

SmartCloud provides a variety of cloud services to enterprise customers. They have datacentres located in Scotland, Asia, and North America.

SLA Terms

SmartCloud offers a choice of SLAs, with different terms depending on what the customer chooses in terms of deployment options. All plans assume the use of multiple instances within each datacentre, so these plans are only concerned with loss of a whole datacentre. Customers wishing to use only a single instance of a service are limited to best effort service, and do not come under any plan.

- Plan A customers deploy their services to two or more of the three datacentres. They are given assurance of high availability, rapid restoration, and compensation for outages of more than an hour.
- Plan B customers deploy their service to their local datacentre, but also allow their data to be regularly replicated in encrypted form to one of the other datacentres, so that their service can be resumed in the event of a local outage. They are given assurance of medium availability, and service restoration within 6 hours, though with possible (temporary) loss of recent activity.
- Plan C customers deploy their service to a single datacentre, and accept the risk of service interruption in the event of an outage. They are given assurance of best-effort service restoration, with a guideline of 24 hours to recover.

Planned Outage Notification and Reporting

SmartCloud finds a structural fault in the building of their US datacentre. To fix this fault and make the building safe, they will need to shut down a large part of the equipment while the work is being done.

Warnings are posted through the customer management interfaces describing the situation and the mitigations being put into effect, along with providing pointers to current status information. This information is placed on the company website, in the customer support system, and by direct notification to the customers by email with sufficient warning time for the customer to take whatever action they need.

Where allowed(Plan A and Plan B), workloads are shifted to other datacentres for continued customer service, with somewhat inferior latency and performance.

Once the building work is completed, the systems are brought back up and normal service resumes.

Unplanned Emergency Outage Response and Reporting

A building contractor working to lay new water pipes near the SmartCloud datacentre in Scotland is working through the night to complete a contract. One of their excavator crew makes a mistake with the routing of a trench they are digging, and as a result they accidentally dig right through some major conduits that carry local telecoms fibres and cables, breaking all the links. The building contractors do not immediately notice the damage they have caused.

Although SmartCloud had purchased diverse physical routing from their telecom supplier, they were unaware that the fibres which left their premises in different directions actually came together

further down the road (at the site of the break). Other services that are also cut include landline telephone cables and links to cellular base stations. The area is mostly isolated from the global communications networks.

Alarms go in the SmartCloud datacentre, reporting that the internet connection is down and all traffic is being lost. On-site staff attempt to contact their head office and the other datacentres with no success – even their cellphones are not able to make calls or send data.

Customers start to notice the outage as their applications begin to fail. Those on Plan A failover to the other SmartCloud datacentres and are able to continue working, while the others must wait for news and advice.

SmartCloud HQ in London sees the breakdown in their telemetry and management from the Scottish datacentre, and start making enquiries as to cause and effects. Their emergency response team are woken up and called in to coordinate the response.

SmartCloud HQ already maintained extensive contact information for their customers, so that they are not dependent on the cloud system itself for all their communications. This includes email addresses, and phone and text message contact information for departments and/or nominated individuals at each customer company.

The emergency response team starts proactively messaging and calling customers who are likely to be affected by the outage. This is complicated by the hour, and the lack of ICT connections to the cloud management service in Scotland. The emergency response team also triggers a prepared public relations plan to notify appropriate news outlets (including relevant social networks such as Twitter) and begins managing the PR situation.

As dawn breaks, the cause of the situation becomes clear. Fixing the connections will require a major telecoms rebuild. The telecom company is able to provide temporary basic connectivity, but far less capacity than the original fibre connections until new fibre can be laid.

More customers become aware of the problem, either from their own systems, the Twitter feed, or direct communications from the CSP. SmartCloud have their website updated with current incident news, and their call centre is able to give constructive advice. Social networks carry pointers to this information.

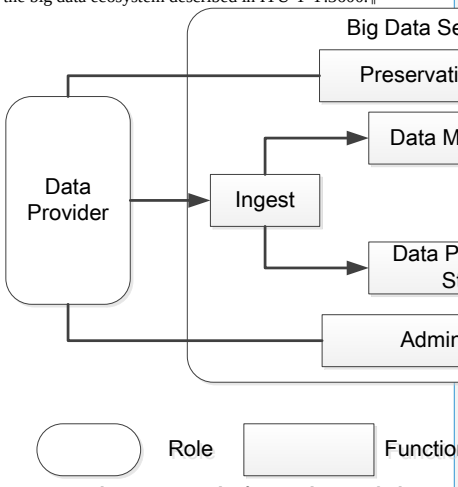
Some Plan C customer realise they could be faced with a significant service interruption, so choose to switch to Plan B or Plan A rather than wait. However, this will take time since the VMs and data in Scotland must be extracted and sent to the other datacentres before it can be made live.

Gradually things return to normal. SmartCloud offer to provide some compensation for lost service, but refuse to accept liability since the outage was caused by factors outside their reasonable control. However, they do launch a lawsuit against both the telecom company (because of the fibre routing) and the building contractor (for causing the damage despite accurate information being available), and provide appropriate details of the incident and their response to their service regulator.

-

Living list #2: Proposed content for clause 8 and 9 of Y.CCICTM

Deleted: Living list #2: Framework of big data preservation¶
This material proposed to add a new sub-clause "6.3 Framework of big data preservation" in Y.BDDP-reqts which described roles and functional entities to support big data preservation. This material is useful for future work of draft Y.BDDP-reqts, however needs more use cases to discover functional entities. Put on the living list at the moment. Framework of BD data preservation needs to be harmonize with BD management framework (see work programme of Q17/13).¶
¶
6.3 Framework of big data preservation¶
This clause describes a framework which includes roles and functional entities to support big data preservation, based on the big data ecosystem described in ITU-T Y.3600.¶



Comments: There are some roles/functional entity which should move after use cases. Otherwise, figure is confused. BD could be replaced by data on high-level view. Usually, we starts from use cases, next requirements and capabilities ...

Deleted: Living list #3: Cloud service evaluation index¶
This material proposes to add a new sub-clause "6.3 Cloud service evaluation index" in Y.CCICTM. It starts discussion about "reputation/evaluation" in inter-cloud environment. At the moment, there are several doubts related to future direction and objectives to reach. First, gap analysis as well as positioning against existing and/or on-going works in others SDO's is needed.¶
6.3 Cloud service evaluation index¶
The reputation of a CSP is highly correlated with the evaluation of cloud services it provides. Cloud service evaluation index could provide a standardized method for evaluating a cloud service. Cloud service evaluation index is a set of categories and attributes. It is designed to help organizations measure cloud services based on their specific business and technology requirements.¶
Comments: First all off we should consider on-going works over other SDO's (e.g. ISO) to provide baseline for future discussion. The required definition should be evoked here. The metric is described in ISO/IEC 19086-2. Second, we should determine what is CSEI and who is in charge of this as well as who evaluates whom. Third, the term "CSEI" shou ...

Deleted: 4

8. Functionalities for managing isolation and security mechanism

[Editor's note:] This clause provides description of functionalities for managing isolation and security mechanisms

8.1 Data Privacy

The cloud service providers should promise that the user data is encrypted or isolated to guarantee that the all the users' data in the same resource pool are not visible to each other. And the cloud service providers is able to access the user data, only when the authorization of user is obtained by the cloud service providers. Its normative description should include the following information:

- According to different cloud services, define the type of data, such as object files, virtual machine images, database, source code, and user logs.
- Declare what technology is utilized to guarantee that all the users in the same resource pool are invisible to each other, e.g., network isolation or encryption algorithms.
- Explicitly what kinds of user data can be accessed by the cloud service provider based on the characteristics of different cloud services.
- Explicitly inform users of the way by which the cloud services provider accesses the users' data.
- Should be able to record the related operation of the operation and maintenance personnel.

Example 6: the service provider can provide the X data encryption algorithm and the Y data isolation method to guarantee that the all the users' data in the same resource pool is invisible to each other.

8.2 Operation and Maintenance Safety Management

The cloud service providers should provide security measures to guarantee the security operation of the management platform. Its normative description should include the following information:

User management: is used to create, modify, delete users or user groups, as well as assign different roles and permissions. And it also can support for user password and certificate information modification.

Cloud account management: allows administrators to manage and authorize all cloud accounts, as well as perform the real-time tracking cloud account resource and cost information in a centralized manner.

Log analysis: refers to the collection and analysis of the complete operating record of the operation and maintenance personnel.

Auditing: audit all the operation behavior of the operation and maintenance personnel.

9. Requirements for inter-cloud trust management

[Editor's note:] This clause provides requirements for inter-cloud trust management based on relevant use cases proposed in Appendix I.
[Editor's note in November 2016] This introduction comes from Orange's contribution (C-06).

This clause provides requirements for data use in inter-cloud derived from the use cases described in Appendix II.

[Editor's note in November 2016] The requirements for inter-cloud trust management are derived from use case on trusted network function virtualization after Orange's contribution (C-06).

It is recommended that CSP provides specification of policies and credentials used for trust management system.

9.1 Data Migration

The cloud service provider should guarantee that the users can control the migration of data,

and guarantee that user Data is able to be moved in and moved out, when the cloud service is enabled or discarded. Its normative description should include the following information:

- According to different cloud services, define the type of migration data based on the definition of Data, such as object files, virtual machine images, database, and source code.
- Specify the data formats supported by different cloud service migrations:
- cloud hosts need to specify the supported image formats, such as image templates (OVF);
- the database needs to specify the supported database format;
- The development platform needs to specify the supported code formats.
- other cloud services.

If only a special format is supported, then whether there is some technology for transforming to the standard format should be clearly specified.

whether there is convenient technology for moving in and out of the user data or not, while maintaining maximum compatibility with user data, such as data storage mode, virtual machine configuration and application data, should be clearly specified.

Example 5: when the user data is moved in or out, the services provider can provide the convenient transforming technology to transform the X format data service or the other storage mode of user data to the Y format.

9.2 Service Resource Management Capability

The cloud service provider should support the customers to expand or reduce the storage time and maximize the storage capacity. Its normative description should include the following information:

- According to the cloud service, declare the types of resources that are expanded or reduced, e.g., computing, storage, bandwidth, minute quotas, and number of concurrent users.;
- Specify the dimensions and units of the resources, which are able to be expanded or reduced, e.g., GB, Gbps, user numbers, and number of CPU kernels.;
- Specify whether the online manner or the offline manner is supported for resources expansion or reduction. If offline manner is supported, then how long time is required for the offline manner is needed to be further introduced.
- Specify the speed of expansion or reduction of resources. If the expansion speed has no threshold, then the specific speed of expansion and speed reduction should be given. However,If there is a threshold of expansion , then the expansion and reduction speed above the threshold is needed to be given.
- there should be the maximum and minimum expansion or reduction capacity, where the maximum expansion or reduction capacity at a time is X and the corresponding minimum value is Y.

Example 11: service providers promise that user can obtain 20% of the computing resources capacity in 24 hours and 100% of the capacity in 2 days. However, the maximum expansion capacity at a time is 100% of all the capacity and the minimum value is 10GB.

It is recommended that CSP implements trust management system to evaluates whether the provided credentials satisfy the specified policy.

9.3 Resource Management

Service provider should be able to manage all of the virtual machine, storage, image, network and other resources on the cloud platform. Its normative description should include the following information:

- Computing resources: refer to supporting the creation, configuration, destruction of virtual machines, startup /shutdown of virtual machines, virtual machines, and clusters.
- Storage resources: refer to supporting the creation, mount, and configuration of virtual volumes.

- Image resource: refers to the ability to support creation, configuration, clone image, and cancellation of image resource.
- Network resources: refer to the functions of supporting bandwidth configuration, load balancing, creating and configuring private networks, creating VPN channels, and so on.
- Resource importing: refers to supporting the import of public, private, or mixed cloud resources.
- Policy management: refers to supporting the cloud resources allocation via automated configuration.

Resource pool management: refers to the support for creating and configuring multiple cloud resource pools.

Living list #3: Proposed new WI "Predictive Fault and performance management to ensure carrier grade reliability and availability of virtual network services on multiple clouds"

Keywords: Multiple cloud, predictive fault, performance management

Abstract: This contribution proposed new work item on "Predictive Fault and performance management to ensure carrier grade reliability and availability of virtual network services on multiple clouds"

[Meeting's note:] There is a lack of A.1 justification as well as skeleton required for new work item. The meaning of FCP (Fault Configuration Prediction) could provide misleading here.

[Meeting's note:] Limitation to NaaS could be too much restricted for large carrier provider, as well as limited to core/transport network services with excluding access network like radio or mobile part of the network. There is a proposal to revise title for "End-to-end faults and performance management in multi-cloud NFV deployments". The "NFV deployments" do not to be highlighted here, as Y.3515 provides NaaS capabilities. There are a several on-going work item or existing Recommendation in Question 18/13 and Question 19/13 which partially addressed these topic. The gap analysis is need to move forward.

Background:

Cloud Computing is being studied in the Telecommunication Engineering Center (TEC) of the Department of Telecommunications (DoT) under Ministry of Communications, Govt. of India, collaboratively in the divisions of Future Networks, Information Technology, Mobile Technologies and Telecommunications Security. Among themselves these divisions are engaged in the study of cloud computing as an essential paradigm for 5G, placement of virtual network functions on clouds and security in virtual network services deployment on multiple clouds. The Future Networks division is presently coordinating the activities. National working group (NWG) - 13 was formed in TEC to coordinate ITU-T SG-13 related activities in India. It is having members from Industries and the Government.

Proposal

This contribution relates to deployment of telecommunication network services over multiple clouds. It proposes to discuss the paradigm of end-to-end fault and performance detection and localization in cloud based virtual network services as a means to achieve carrier grade reliability and availability. The proposal is generic in nature and is applicable to all member states.

[Meeting's note:] The meaning "end-to-end" have to be clearly describe here to avoid some future doubts.

The details of new work item are as per the Annexure A attached.

Annexure A

Use case:
[Meeting's note:] Use case should be provided in proper form, if apply to scope of work.

1. Title of the use case
a) Name of the use case: Predictive Fault and performance management to ensure carrier grade reliability and availability of virtual network services on multiple clouds.
b) ID of the use case:
c) Version/revision history: 22/October/2017

2. Source: India/ MoC/ TEC Objective of the use case
This use case describes the problem of fault and performance management in telecommunication networks deployed over clouds, specifically multiple clouds. Such a deployment introduces complexities beyond IT services deployment over clouds where problems can be traced to virtual machines or the

physical infrastructure underlying virtualization. In virtual network services the virtual network functions may themselves randomly malfunction in addition to the already existing complexities in multi-cloud deployments. Identification of the fault and performance problem and elements of the solution would help in reaping myriad benefits that such deployments could potentially bring.

3. Background
a) Countries' specific telecommunication network deployment scenario
The India specific information is available here http://www.dot.gov.in/telecom-glance
The use-case described here is generic in nature and applicable to all member states interested in ushering state-of-the-art cloud based telecommunications network deployment in their countries. Such deployment are expected to give a number of benefits over traditional deployments using physical applicances. Some of the benefits are: flexibility of obtaining resources, ease of scaling and descaling, freedom from proprietary hardware and software, ease of redeploying resources, risk mitigation, ease of deploying new services and reduced total cost of operation.

b) Current Practice
The current practice largely involves use of physical network applicances like routers, switches, broadband remote access servers or middleboxes like firewalls, deep packet inspectors or load balances. These appliances and associated software are normally proprietary and leads to vendor lock-in making expansions and deployment of new services difficult and time consuming. They are also not amenable to easy scaling or redeployment of resources. The power and space requirements as well as the total cost of operation is higher in physical networks.
In traditional networks described above, time-tested standards relating to fault, configuration, accounting, performance and security (FCAPS) are embodied in ISO Common Management Information Protocol (CMIP) and ITU TMN M.3010 and M.3400 recommendations. Network management based on relevant standards provides five nines availability and carrier grade reliability.
[Meeting's note:] Citation like here related to ISO's matter or ITU-T Recommendations need to be referred directly.

c) Need for Use Case
Network function virtualization (NFV) is a promising framework. NFV coupled with multi-cloud computing provides numerous advantages to the service providers including ease of deployment, ease of scaling, ease of introducing and switching off services and reduced cost of operation. This would increase viability of telecommunications business and lead to a thriving telecommunication sectors in the member states. NFV over multiple clouds has not yet attained the level of performance to be a viable replacement

for traditional networks. One of the main reasons is the absence of a standard based Fault, Configuration, Accounting, Performance and Security (FCAPS) framework for the virtual network services. Since deployments of such networks are in nascent stages in various countries, there is a need for standardization of techniques for fault and performance detection and localization in such networks.

d) Ecosystem Specifics

Some of the key challenges in NFV over multi-clouds are as follows:

• Absence of an FCAPS framework
• Non-applicability of traditional rule based techniques used in today's networks
• Multiple layers of implementation: physical infrastructure, NFVI (Virtual Machines), Virtual Network Functions (VNF) and Virtual Network Services.
• Massive distribution of network functions over disparate clouds
• Multiple control centers: cloud management systems, operators' OSS/BSS and NFV-MANO (Management and Orchestration)

4. Description

a) Summary

Telecommunications networks have traditionally been designed to provide five nines availability and standards based quality of service. In virtual network services deployment over multiple clouds it is challenging to equip multi-cloud management systems to deal with fault and performance issues. Virtual network services have underlying physical and network function virtualization infrastructure. The telecommunications network functions in the virtualized form go into the virtual machines provided by the NFVI. When performance deviates from normal or a fault occurs, there is no access to the physical hardware for telecom operators to test. The root cause of the problem could be in the physical, virtual layer or the virtual network functions. The traditional deterministic methods fail to deliver in virtual environments in which virtual resources can be constantly scaled, migrated or destroyed. It is proposed to make use of predictive techniques to be able to identify fault or performance issues before or after they have occurred.

b) Scope

This Recommendation is intended to facilitate effective end-to-end fault and performance management in multi-cloud virtual network services. In telecommunication networks with physical appliances, deterministic methods ensure carrier grade availability and reliability. However, when telecom service providers service function chains using virtual resources over multiple clouds a number of complex factors make it imperative to use predictive methods for assuring carrier grade availability. This recommendation discusses open source non-discriminatory procedure to ensure this objective.

[Meeting's note:] It is required to use cloud computing vocabulary under WP2/13, therefore "telecom service provided" should be replaced by "cloud service provider". Please be aware of cloud notation, see ITU-T Y.3500, Y.3501 and Y.3502.

[Meeting's note:] The scope of work should be very clear and reflects intention of Recommendation. We found preliminary agreement on first items as "overview of end-to-end faults and performance management in multiple-clouds" or "fault/performance detection model", but other are needed to determine direction of this new work item, e.g. framework, requirements, methodology, etc. The use case illustration with clear boundaries are expected to define scope of work. Please check SG2 work as well , as some of documents related to cloud and non-cloud environment should be useful.

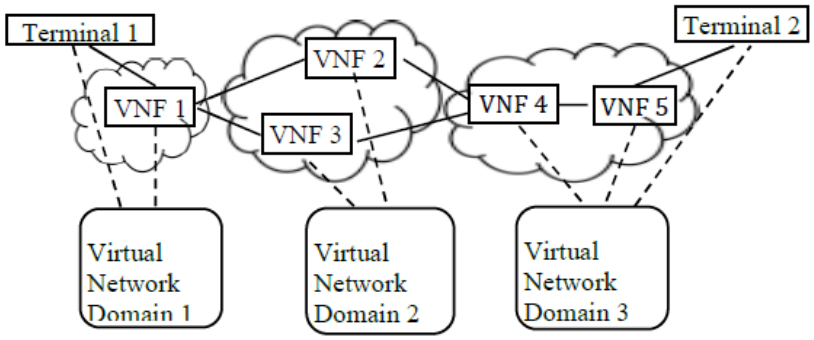
c) Ecosystem Description

Network Function Virtualization (NFV) provides the advantages of breaking free from proprietary network appliances and brings in ease of scaling. When NFV is deployed over multiple clouds then there are added advantages like greater flexibility in obtaining resources, avoiding total outages, proximity to customers and lower total cost of operation. Cloud technology can multiply the benefits of NFV [2], [3], [59]. It could provide greater flexibility in obtaining resources, bring Network Service Provider's (NSP's)

points of presence close to customers, provide an opportunity to optimize performance and control cost. However, NFV over multiple clouds has not yet attained the level of performance to be a viable replacement for traditional networks. One of the main reasons is the absence of a standard based Fault, Configuration, Accounting, Performance and Security (FCAPS) framework for the virtual network services. Traditional networks have time-tested standards relating to fault, configuration, accounting, performance and security (FCAPS) as embodied in ISO Common Management Information Protocol (CMIP) and ITU TMN M.3010 and M.3400 recommendations. In NFV Concerns regarding five nines availability and quality of service parameters, like latency and packet loss, still remain.
In NFV, faults and performance issues can have complex geneses within virtual resources, compute, storage and networking, as well as virtual network functions and cannot be effectively handled by traditional rule-based systems. To be able to make use of the multi-cloud paradigm effectively, it is important that we fix the FCP issues for this environment. Without a robust mechanism for handling FCP, service providers would find meeting service level agreements (SLAs) difficult and growth of the promising technology of NFV might get hampered. The framework should contain mechanisms for handling manifest and latent fault and performance issues.

i) Network Service Structure
Based on the ETSI specifications and IETF RFC a network service can be described as a service function chain (SFC) or virtual network function (VNF) graph, interconnected by virtual network resources, as an ordered set of VNFs that represent functions like routers and broadband network gateways or middleboxes like load balancers and firewalls, which act on the traffic in the sequence they appear in the chain. VNFs are hosted on virtual machines (VM) instantiated over physical data center and network resources. An example of end-to-end service is shown on the left side of Fig 1.

Fig. 1 Multi-domain End-to-End Service



[Meeting's note:] This figure 1 seems to be a good candidate to illustrate use case as representative illustration of scope of work this Recommendation. The use case of vCPE could be a good starting point here with potential towards change management, policy based management (see draft Rec. Y.ccictm), machine learning support cloud, etc.

Faults happen due to physical or algorithmic causes. They appear as errors. Errors in turn are deviations of a system from normal operations. Errors are reported through system alarms. Alarms are notifications about specific events that may or may not be errors. The degradation of a service can be detected through notifications, counters or meters. The FCP system should be able to identify which issues are potential performance hazards or may result in a fault that would require resources to rectify. Four levels of severity of events have been defined in ITU standard X.733: Critical, Major, Minor, and Warning [ITU92]. The critical alarm comes when the service can no longer be provided to the user. Major alarm indicates the service affective condition while minor means no current degradation is there, but if not

corrected may develop into a major fault. A warning is an impending service affecting fault or performance issue. It is for the predictive capabilities of the FCP system to predict what faults will develop and with what severity levels.
Communication networks are widely distributed and are complex. The variety of FCAPS issues that can afflict them is large. To detect, diagnose and localize any condition that degrades network performance becomes quite onerous. In this contribution we restrict our discussion to:

1. Detection of any condition that has already led to or could lead to degraded performance or failure. The reasons could be manifest faults, hidden faults or inconspicuous deviations. The goal of FCP detection would be to sense and notify impending or actual fault and performance issues.

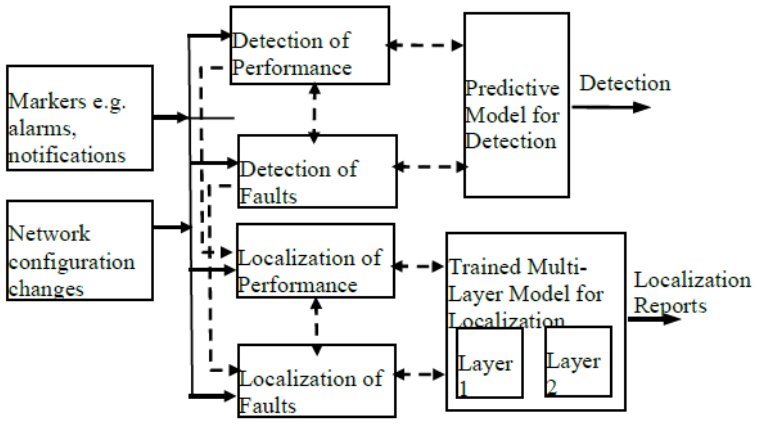
2. Identification and localization of manifest and impending faults. The goal of FCP localization would be to determine the root cause of the problem by identifying the resources that are malfunctioning or the severity with which they may malfunction in the future.

Any fault and performance management system should take into account all the markers including alarms, notifications, warnings, observed behaviour, counter readings and measured values of performance indicators to carry out the above functions.

ii) FCP Solution Components

FCP management in cloud based network services would be a collaborative process among the elements constituting the service and the management systems involved. Modern communication systems produce large volumes of high-dimensional operational data. In such a case, analyzing the data to get an actionable understanding of the situation becomes difficult. In general, the researchers agree on predictive approaches that take a learning route to solve the problem of the complex interaction of features of fault detection and localization.

Fig 2. Fault/Performance Detection and Localization Model



The proposed model has predictive and deductive properties to meet the FCP requirements. Run time monitoring and measurements, alarms, notifications and warnings, configuration changes, measurements and environmental factors are all used along with the models trained with historical data to draw inferences about the manifest performance and fault issues. Additionally, decision about impending faults is taken using these inputs and the predictive properties of machine learning models. The detection system first decides whether there is a manifest or an impending fault or a performance issue. Based on this, the

system will launch into identification and localization. Detection is essentially a two-stage binary classification problem that first classifies the outcome into 'normal performance' and 'abnormal performance' or 'faulty' and 'not faulty' classes. Then for the 'faulty' or 'abnormal' cases, it decides whether the problem is manifest or impending. Failure prediction needs to be accompanied with a high probability of correctness as actions following such a prediction involve cost. For localization, the model uses a multi-layered strategy. First, the broad category of the fault is determined. The system then identifies the actual device(s) having a fault or suffering from performance degradation and their severity levels. Severity of impending faults need deeper predictive structures.

5. **Proposal:**
This contribution is being submitted for the information and benefit of member states. It may be taken in to account in the standardization work plan of future networks involving end-to-end management of cloud computing when applied to telecommunications networks.

_____