

Framework 16.0 Product Conformance Certification Report

**CENX
V6.1**

**Version 1.0
January 2017**

Table of Contents

List of Figures.....	0
List of Tables.....	0
1 Introduction.....	1
1.1 Executive Summary.....	1
2 Product Functionality/Capability Overview.....	2
2.1 CENX Product Overview.....	2
3 Business Process Framework Assessment Overview.....	3
3.1 Mapping Technique Employed.....	3
3.2 Business Process Framework Level 2 Process Scope.....	4
3.3 Product Scope.....	6
4 Business Process Framework – Process Mapping Descriptions.....	7
4.1 Level 2: 1.4.6 - Service Problem Management.....	8
4.1.1 Level 3: 1.4.6.1 - Create Service Trouble Report.....	8
4.1.2 Level 3: 1.4.6.2 - Diagnose Service Problem.....	13
4.1.3 Level 3: 1.4.6.6 - Close Service Trouble Report.....	16
4.1.4 Level 4: 1.4.6.7 - Survey & Analyze Service Problem.....	17
4.1.5 Supporting Evidence References.....	28
4.1.6 Level 4/Level 3 Detailed Scores.....	28
4.2 Level 2: 1.4.7 - Service Quality Management.....	29
4.2.1 Level 3: 1.4.7.1 – Monitor Service Quality.....	29
4.2.2 Level 3: 1.4.7.5 – Create Service Performance Degradation Report.....	37
4.2.3 Level 3: 1.4.7.7 – Close Service Performance Degradation Report.....	40
4.2.4 Supporting Evidence References.....	41
4.2.5 Level 4/Level 3 Detailed Scores.....	41
4.3 Level 2: 1.5.8 – Resource Trouble Management.....	42
4.3.1 Level 3: 1.5.8.1 - Survey & Analyze Resource Trouble.....	42
4.3.2 Level 3: 1.5.8.2 - Localize Resource Trouble.....	50
4.3.3 Level 3: 1.5.8.6 - Close Resource Trouble Report.....	57
4.3.4 Level 3: 1.5.8.7 - Create Resource Trouble Report.....	58

4.3.5	Supporting Evidence References.....	62
4.3.6	Level 4/Level 3 Detailed Scores.....	62
4.4	Level 2: 1.5.9 – Resource Performance Management	63
4.4.1	Level 3: 1.5.9.1 - Monitor Resource Performance.....	63
4.4.2	Level 3: 1.5.9.5 – Create Resource Performance Degradation Report	68
4.4.3	Level 3: 1.5.9.7- Close Resource Performance Degradation Report	71
4.4.4	Supporting Evidence References.....	72
4.4.5	Level 4/Level 3 Detailed Scores.....	72
5	Information Framework Assessment Overview	73
5.1	Mapping Technique Employed.....	73
5.2	Information Framework Assessment - ABE Scope	73
5.3	Product Scope.....	73
6	Framework Conformance Result.....	74
6.1	Business Process Framework – Scoring Rules	74
6.2	Business Process Framework – Conformance Result Summary.....	76
6.3	Business Process Framework – Detailed Conformance Results.....	78
6.4	Information Framework – Scoring Rules.....	82
6.4.1	Information Framework Maturity Conformance Scoring Methodology	82
6.4.2	Information Framework Adoption Conformance Scoring Methodology	82
6.5	Information Framework – Conformance Result Summary	83
6.5.1	Information Framework - Maturity Conformance Result Summary	83
6.5.2	Information Framework - Adoption Conformance Result Summary	83
6.6	Information Framework – Detailed Conformance Result	84

List of Figures

Figure 3-1 Level 2 process coverage for CENX Assessment	4
Figure 3-2 Level 3 process coverage for CENX Assessment	5
Figure 3-3 CENX Service and Resource Assurance mapped to eTOM L2 Processes in scope	6
Figure 6-1 TM Forum Business Process Framework: Conformance Scoring Rules	74
Figure 6-2 Business Process Framework: Conformance Results Service Domain	76
Figure 6-3 Business Process Framework: Conformance Result Resource Domain	77

List of Tables

Table 4-1 1.4.6 Service Problem Management – Level 4 & Level 3 Scores	28
Table 4-2 1.4.7 Service Quality Management – Level 4 & Level 3 Scores.....	41
Table 4-3 1.5.8 Resource Trouble Management– Level 4 & Level 3 Scores	62
Table 4-4 1.5.9 Resource Performance Management– Level 4 & Level 3 Scores	72
Table 6-1 Business Process Framework: Detailed Conformance Results	78

1 Introduction

1.1 Executive Summary

This document provides details of the CENX self-assessment and TM Forum's Conformance Assessment of the **CENX** product, against the following Framework 16.0 components:

- Business Process Framework Version 16.0

The assessment included a review of:

- The methodology approach to process modeling against the TM Forum's Business Process Framework Release 16.0 according to the specific processes submitted in scope for the Assessment.

Note that Conformance to the Information Framework (SID) Aggregate Business Entities (ABEs) was not covered in this Assessment.

2 Product Functionality/Capability Overview

2.1 CENX Product Overview

The CENX portfolio of solutions provides a full suite of software products to significantly improve management of data connectivity services such as IP VPNs, MPLS, Carrier Ethernet, Ethernet Over SONET, and NFV technologies. With CENX, service providers can harness the power of big data analytics and cloud computing to orchestrate and assure inter-provider network services.

CENX provides end-to-end, real-time visualization of all essential Layer 1, Layer 2, and Layer 3 network services, generating the most accurate picture of the services and topologies — from a national or regional view to the service and segment details, including location visuals. By providing the flexibility to contextualize and search the data across different levels of detail and different operational domains, CENX provides a single-pane view for network operations center (NOC) personnel.

CENX analyzes a wide range of data sources to provide powerful service visualization, management and assurance, capacity planning, real-time troubleshooting, and workflow orchestration capabilities, including sophisticated, predictive, real-time and historical analytics. It provides powerful integrated modules to support the management and assurance of network service assets including: Service Visualization, Continuous Data Audit, Automated Reconciliation, Capacity Planning, Workflow Orchestration, Network Analytics, Real-time Troubleshooting, and SLA Management.

CENX's solution is architected to facilitate the transition to NFV and SDN by leveraging open standards and architectures to integrate SDN/WAN controllers and NFV management and orchestration functions into its comprehensive service information model. Using standard APIs, network big data is collected, correlated, and displayed to provide actionable intelligence and automation of the full end-to-end service lifecycle, from service design through provision, test, assure, and disconnect.

CENX's modularized software and services provide a comprehensive, flexible solution that meets the needs of service providers as their needs evolve beyond inventory integrity assurance to service management and assurance, and from physical network and service orchestration to NFV, SDN, and end-to-end LSO.

CENX transforms network big data into real-time actionable intelligence. CENX accelerates end-to-end operations by harnessing dynamic analytics and web-scale computing to visualize, manage and assure data services across multi-vendor, SDN and NFV networks.

3 Business Process Framework Assessment Overview

3.1 Mapping Technique Employed

Business Process Framework Level 4 descriptions are analyzed by looking for implied tasks. (This is similar to how process decomposition can use Semantic Analysis). Each Business Process Framework process is supported by descriptive text. In many cases, each process is aligned and mapped to appropriate company documentation references solution, methodology or modeling material.

Note that when a Level 3 process has not been decomposed to Level 4 processes, the implied tasks for the given Level 3 process are analyzed.

The Business Process Framework Level 4 descriptions (or Level 3 if appropriate) are analyzed by looking for implied tasks. Color coded text as highlighted below is used as part of the process mapping whereby highlighted text indicates the level of support for a Level 4 process implied task:

- **GREEN** is used to highlight key words or key statements that are fully supported
- **YELLOW** is used to highlight key words/key statements that are partially supported
- **GREY** is used to highlight key words/key statements that are not supported
- No highlighting is used for words/statements that are irrelevant, just for reference or needed to complete the sentence.

Manual and Automated Support

It is important to determine whether the implied task is supported by manual steps, automated steps, or a combination of both. In this document, “A”, “M”, or “AM” is used for each task to indicate that the step or steps is/are automated (A), manual (M), or both (AM).

TM Forum Note 1: *When process mappings are presented against Level 4 processes, the mappings are provided against the text in the “Mandatory” field for the process. In the event of the Mandatory field not being used, the process mappings are in that case provided against the Level 4 Brief/Extended descriptions.*

TM Forum Note 2: *Note that if a Level 3 process has not been decomposed to Level 4 processes in the Business Process Framework, in such cases the process mapping support is provided against the Level 4 process descriptions (Brief & Extended).*

3.2 Business Process Framework Level 2 Process Scope

The following figure represents the Business Process Framework Level 2 processes (high-lighted in green) that were presented in scope for the assessment and that were assessed and support the corresponding Business Process Framework processes according to the results in Chapter 6 Framework Conformance Result.

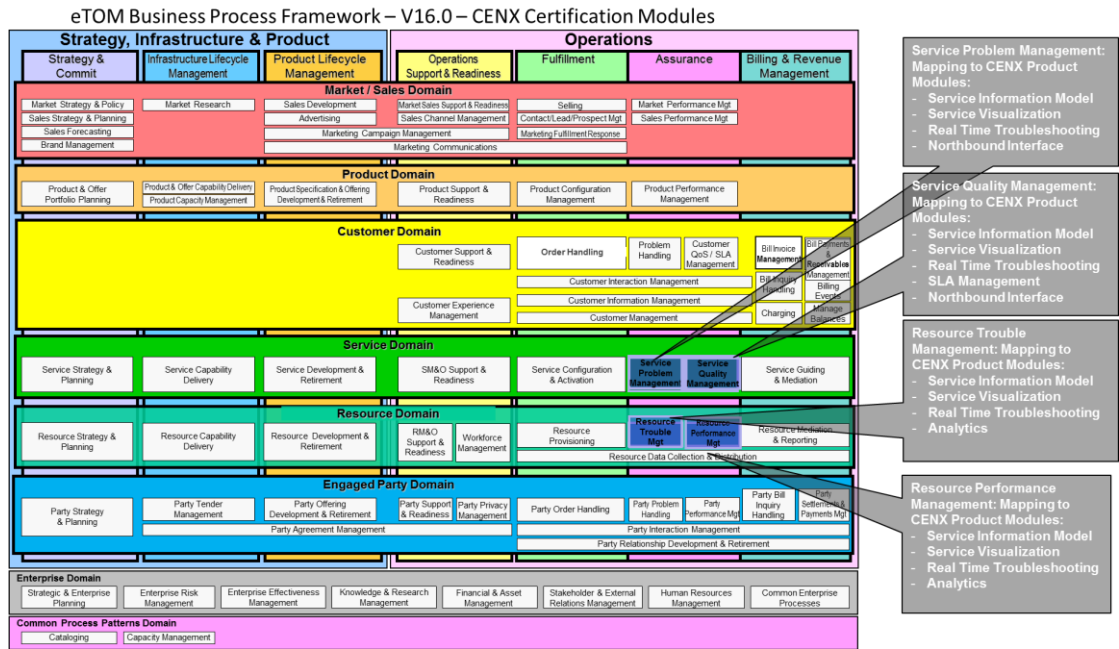


Figure 3-1 Level 2 process coverage for CENX Assessment

The following diagram identifies the number of Level 3 processes that were submitted for assessment, for each Level 2 process that was submitted in scope for the Assessment.

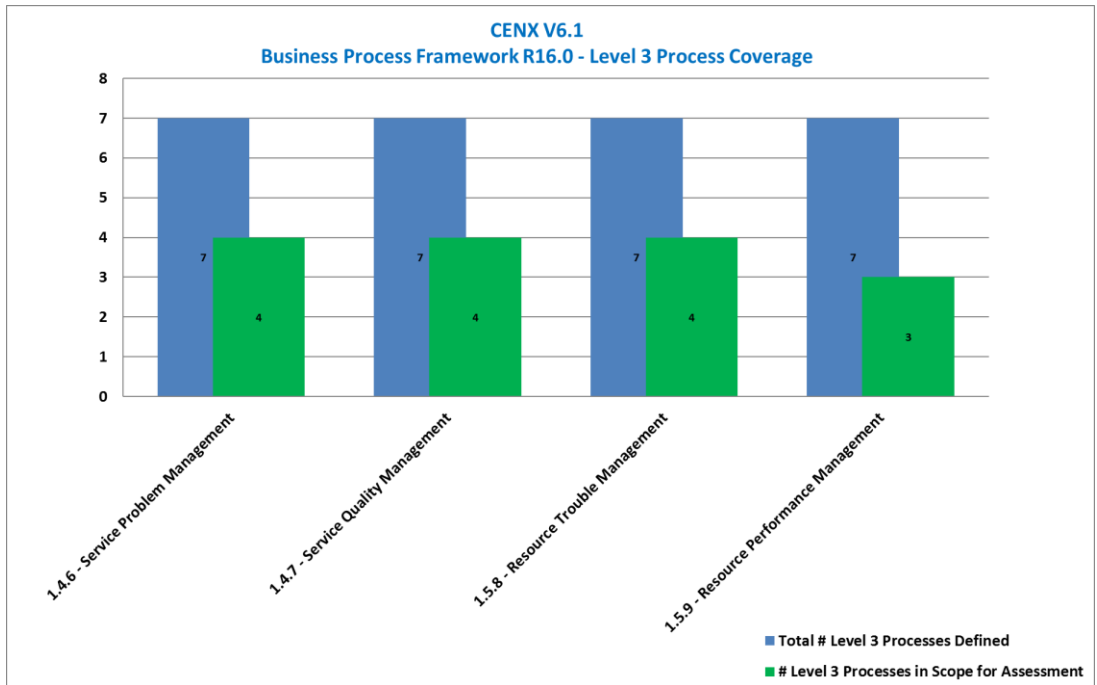


Figure 3-2 Level 3 process coverage for CENX Assessment

3.3 Product Scope

The following diagram represents the CENX product with mappings to the Business Process Framework Level 2 processes that were submitted in scope for the Conformance Certification assessment.

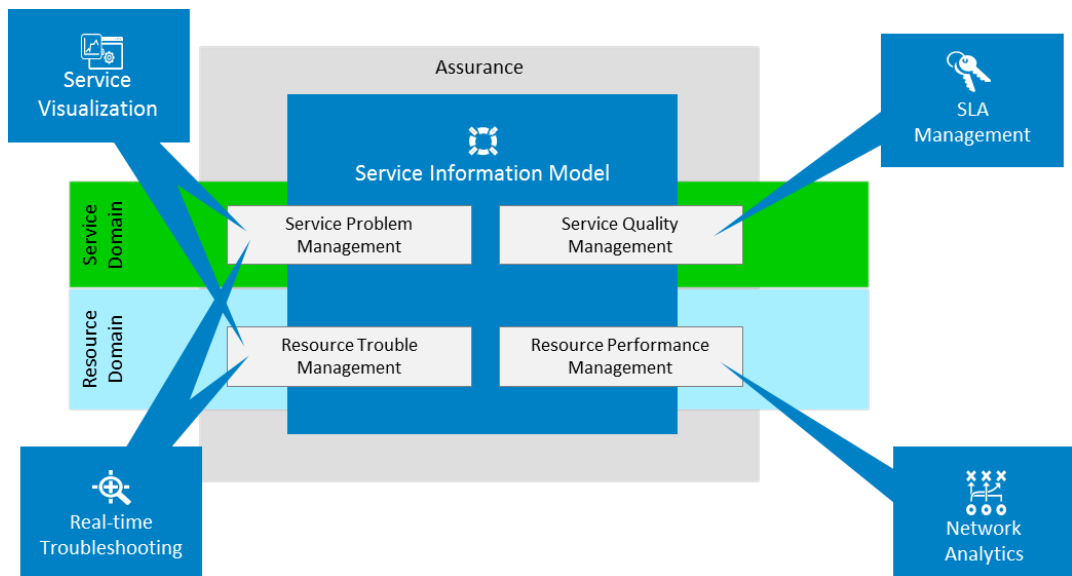


Figure 3-3 CENX Service and Resource Assurance mapped to eTOM L2 Processes in scope

4 Business Process Framework – Process Mapping Descriptions

This Section provides the Process Mapping output from CENX self-assessment which was reviewed by TM Forum Subject Matter Experts alongside supporting documentation for the CENX product.

4.1 Level 2: 1.4.6 - Service Problem Management

4.1.1 Level 3: 1.4.6.1 - Create Service Trouble Report

LEVEL 3 PROCESS MAPPING DETAILS 1.4.6.1 - Create Service Trouble Report
Brief Description: Create a new service trouble report.
Extended Description: <p>The objective of the Create Service Trouble Report process is to create a new service trouble report. <A1></p> <p>A new service trouble report may be created as a result of service alarm event notification analysis, and subsequent creation of new service alarm event records, undertaken by the Survey & Analyze Service Problem processes<A2>, or at the request of analysis undertaken by other processes in the Customer (in particular a Customer Problem Report can generate one or more Service Trouble Reports), Service or Resource Domains which detect that some form of failure has occurred for which service restoration activity is required to restore normal operation<A3>.</p> <p>If the service trouble report is created as a result of a notification or request from processes other than the Survey & Analyze Service Problem processes, the Create Service Trouble Report processes are responsible for converting the received information into a form suitable for the Service Problem Management processes, and for requested additional information if required. <A4></p> <p>These processes will make estimates of the time to restore service which will be included in the new service trouble report so that other processes can gain access to this information <M1>.</p> <p>CENX Compliance</p> <p>One of the key functions of the CENX Service Intelligence Suite is to recognize faults in the network, correlate the faults to the corresponding network elements, filter sympathetic messages, determine the impact of the fault against customer services, and to generate tickets for the derived fault so that actions can be performed to resolve the fault. CENX highlights the services that are impacted by each problem and shows all problems affecting a given service.</p> <p>A service trouble report within CENX provides visualization of a service, highlighting the service monitoring status, and the set of problems that have been detected that are having an impact on the customer. A corresponding perspective is to show a problem or event and the corresponding services impacted by that problem. The monitoring status for the service is shown as 'ok' for no impacting problems, 'warning' for potential problems but the service is still being delivered for</p>

'failure' where the service is severely impacted.

In the reference documentation with supporting screenshots (SS 4.6.1), we demonstrate the service trouble report with two perspectives:

- screenshot 1 shows for a given service showing the aggregated status impact on this service and all associated alarms/troubles;
- screenshot 2 shows for a given alarm/trouble the list of all services impacted;
- screenshot 3 shows another perspective on the Service Troubles showing all troubles and the impacted services. <A1>

An alarm/event/trouble can be identified and provided to CENX by any application and ingested into the CENX Real-Time Troubleshooting module for processing and subsequent service trouble reporting. The following excerpt from our Product Description describes this showing support for A2/A3.

Please reference CENX Product Description - Section 2.5.1:

An average tier 1 service provider network processes a million events per minute, with data coming from multiple independent systems, tools, and organizations. The volume and disparate sources of data present challenges in correlating the data to effectively detect issues, and isolate faults to the circuit path and access provider.

With CENX Real-time Troubleshooting, network and service operations teams can view correlated alarms and events to Sectionalize faults within a single system.

CENX monitoring and Real-time Troubleshooting:

- *gathers and displays network alarms and monitoring data from network devices and third-party applications. In support of item <A3>, the alarm, trouble or event may be ingested from any application.*
- *applies fault correlation logic to determine and display the root cause fault and associated dependencies*
- *applies the alarm and fault correlation data to the visualization of the audited and verified network*
- *displays utilization and monitoring graphs and events at the path level*
- *integrates with third-party systems to streamline workflow processes*

CENX displays near real-time network monitoring information in the Network view, Monitoring Dashboard, Paths view, and Port View.

For each service event identified, CENX will correlate the event, identifying the trouble and initiate service problem management processes to resolve it. As can be seen in supporting screenshot #1 for this Section, BMC Remedy tickets have been created and referenced to the issue. The ticket is created with the source of the problem, the set of services impacted by the trouble and other supplemental information. Clicking on the trouble from the CENX portal would bring you

to the external Problem Management application. <A4>

CENX does not provide out of the box capability for determining the time to restore the service problem. However through configuration and customization, the service problem could be readily extended using data from the CENX data store to determine average resolution time for similar issues and provide an estimated resolution. <M1>

4.1.1.1 *Level 4: 1.4.6.1.1 – Generate Service Problem*

LEVEL 4 PROCESS MAPPING DETAILS 1.4.6.1.1 – Generate Service Problem
Brief Description: This process creates a new Service Trouble report. <A>
Extended Description: Not used for this process element
CENX Compliance: Compliance for this process is described under A1/A2/A3 from 4.6.1 Create Service Trouble Report.

4.1.1.2 *Level 4: 1.4.6.1.2 – Convert Report to Service Problem Format*

LEVEL 4 PROCESS MAPPING DETAILS 1.4.6.1.2 – Convert Report to Service Problem Format
Brief Description: If the service trouble report is created as a result of a notification or request from processes other than the Survey & Analyze Service Problem processes, this process is responsible for converting the received information into a form suitable for the Service Problem Management processes, and for requested additional information if required. <A>
Extended Description: Not used for this process element
CENX Compliance: Compliance for this process is described under A4 from 4.6.1 Create Service Trouble Report.

4.1.1.3 *Level 4: 1.4.6.1.3 – Estimate Time for Restoring Service*

LEVEL 4 PROCESS MAPPING DETAILS 1.4.6.1.3 – Estimate Time for Restoring Service
Brief Description: This process estimates the time to restore service which is included in the new Service Trouble report so that other processes can gain access to this information. <M1>
Extended Description: Not used for this process element
CENX Compliance: This process is not supported out of the box within CENX processes, but it could be configured as described under M1 from 4.6.1 Create Service Trouble Report.

4.1.2 Level 3: 1.4.6.2 - Diagnose Service Problem

LEVEL 4 PROCESS MAPPING DETAILS 1.4.6.2 – Diagnose Service Problem
<p>Brief Description:</p> <p>Identify the root cause of the specific service problem, including those service problems related to security events.</p>
<p>Extended Description:</p> <p>The objective of the Diagnose Service Problem processes is to identify the root cause of the specific service problem. These processes are invoked by the Track & Manage Service Problem processes.</p> <p>The responsibilities of these processes include, but are not limited to:</p> <ul style="list-style-type: none">• Verifying whether the service configuration matches the appropriate product features; <A1>• Performing diagnostics against the specific services; <A2>• Running tests against the specific services; <A3>• Starting and stopping audits against specific services• Scheduling routine testing of the specific services. <p>The Diagnose Service Problem processes will make the results of the root cause analysis available to other processes. The Diagnose Service Problem processes will update the open service trouble report, as required during the assessment, and when the root cause has been identified. <A4></p> <p>When the process is complete the Diagnose Service Problem processes will notify the Track & Manage Service Problem processes. <A5></p>
<p>CENX Compliance</p> <p>CENX is designed to recognize service problems quickly and efficiently and determine the root cause of that problem by automating the recognition of principal alarms (from the noise of sympathetic alarms) and enabling manual interactions for further troubleshooting and service problem resolution.</p> <p>CENX starts the process by building and maintaining an accurate service topology including a regular audit of all network configurations and relating these to the definitions of the services from customer and service inventory applications and represented in the CENX Service Information Model (SIM). Service Configuration errors are recognized in the solution through the build and audit process as described in the Product Description (Section 2.3). (A1)</p> <p>Events and Alarms are continuously ingested from network elements, EMS's, and test drivers by CENX's Real-time Troubleshooting (RTT) module which builds and maintains a fault tree which is correlated to the data from the CENX SIM to allow for the determination of principal versus</p>

sympathetic alarms. As alarms are received, classified, updated and closed, events are published on the northbound interface and may be orchestrated through a business process using the workflow manager. (A4/A5)

Test results, performance data and utilization data is continuously ingested by CENX's Network Analytics and SLA Management modules and correlated against the SIM data. CENX continuously analyses this data to determine if service problems exist, and if so an alarm is generated and posted to the Real-time Troubleshooting module. (A2)

Each of the test results is compared against the network element and subsequently the specific service constituted and supported by those network elements. For example, a test driver using TWAMP, ping, or other non-intrusive tests as described in Section 2.6.2 of Product Description are associated with the applicable resource and appropriate service in question. (A3).

CENX performs big data analytics upon all performance and utilization data and presents these analytics in a comprehensive set of dashboards and reports within the CENX Service Portal. This data is available through extracts, event notifications through the Northbound interface, or through a set of query transactions. Please see Product Description Section 2.6.4 for details (A4)

4.1.2.1 *Level 4: 1.4.6.2.1 – Verify Service Configuration*

LEVEL 4 PROCESS MAPPING DETAILS 1.4.6.2.1 – Verify Service Configuration	
Brief Description:	This process verifies whether the service configuration matches the appropriate product features. <A>
Extended Description:	Not used for this process element
CENX Compliance:	<p>The CENX Continuous Data Ingest and Audit processes, ingest data from the network elements involved in the delivery of a service to the customer, stitching the configurations together and comparing the results to various data sources from the BSS/OSS to ensure that a complete picture of the service topology is realized and that the configurations are consistent between the actual network and the specific OSS. Each topology is given a build and audit score. the build score is based on the completeness of the service and network configuration. The audit score compares the service/network configuration with that from the OSS inventories.</p> <p>The topology build is described in Product Description Section 2.2 and the process of auditing the data across data from various BSS/OSS systems is described in Section 2.3.</p>

4.1.2.2 *Level 4: 1.4.6.2.2 – Perform Specific Service Problem Diagnostics*

LEVEL 4 PROCESS MAPPING DETAILS 1.4.6.2.2 – Perform Specific Service Problem Diagnostics	
Brief Description:	This process performs diagnostics against the specific services. <A>
Extended Description:	Not used for this process element
CENX Compliance:	<p>CENX interoperates with various test probes and other test harness applications such as TWAMP, ICOMP, Performance Monitoring, and Service Performance Monitoring applications as described in the Product Description Section 2.6.2.</p> <p>Test results from these applications are ingested into CENX and associated with the resource or service to which the test applies.</p> <p>Custom tests can also be readily configured to be launched from the CENX visualization portal. As can be seen in the reference document screenshots (SS4.6.2), from the view of a network service, one can launch and perform an immediate test for the given service.</p>

4.1.3 Level 3: 1.4.6.6 - Close Service Trouble Report

LEVEL 3 PROCESS MAPPING DETAILS 1.4.6.6 – Close Service Trouble Report
Brief Description: Close a service trouble report when the service problem has been resolved.
Extended Description: The objective of the Close Service Trouble Report processes is to close a service trouble report when the service problem has been resolved. <A1> These processes monitor the status of all open service trouble reports, and recognize that a service trouble report is ready to be closed when the status is changed to cleared. <A2>
CENX Compliance The CENX Real-time Troubleshooting module manages events, problems and alarms that are generated for each network element and associates these events to the services these resources constitute. Each event has a managed state and with each change in state, a northbound message is generated through the Northbound Interface. These events may also be orchestrated by the Workflow Manager where they are coordinated through a business process of manual and automated tasks. The monitored status of the service itself is aggregated status of all alarms/events/problems that impact this customer's service. When the state of an event/alarm is resolved, the state of any impacted services is reassessed based on any other existing alarms affecting those services. When the monitored state changes from failure to ok, this indicates that the service problem is resolved. <A1> The service reports no longer show the problem and a state change message is published to any interested applications. <A2> Section 2.5.1 of the Product Description shows the event processing. Section 2.5.2 shows the message that is generated for external applications when the monitored service state changes including when the service changes from failure to ok. The screenshot reference document (SS4.6.1) shows the service monitoring status and the corresponding events/alarms.

4.1.4 Level 4: 1.4.6.7 - Survey & Analyze Service Problem

LEVEL 4 PROCESS MAPPING DETAILS 1.4.6.7 – Survey & Analyze Service Problem
Brief Description: Monitor service alarm event notifications and manage service alarm event records in real-time. Service alarm events include security event alarms.
Extended Description: The objective of the Survey & Analyze Service Problem processes is to monitor service alarm event notifications and manage service alarm event records in real-time. <A1> Responsibilities of the Survey & Analyze Service Problem processes include, but are not limited to: <ul style="list-style-type: none">• Detecting and collecting service alarm event notifications; <A2>• Initiating and managing service alarm event records; <A3>• Performing service alarm event notification localization analysis; <A4>• Correlating and filtering service alarm event records; <A5>• Reporting service alarm event record status changes to other processes; <A6>• Managing service alarm event record jeopardy conditions. <Not supported> Service alarm event notification analysis encompasses the identification of the service alarm event in terms of reporting entity and nature of the service alarm event. It will then analyze the service alarm events based on a number of criteria and then suppress redundant, transient or implied service alarm events by means of filtering and correlation. <A8> It includes the notification of new service alarm event records, or status changes of previously reported service alarm event records, <A9> as well as abatement messages when service alarm event records have been cleared. <A10> The analysis will correlate service alarm event notifications to planned outage notifications to remove false service alarm event notifications arising as a result of the planned outage activity. <Not Supported/Future> These processes may determine that a service alarm event notification may represent a customer impacting condition. In these circumstances this process is responsible for indicating a potential customer problem to the Problem Handling processes. <A11> As a part of this

indication this process is responsible for identifying the impacted deployed product instances associated with the service instances presenting alarm event notifications and passing this information to the Problem Handling processes. <M1>

Service alarm event record correlation and filtering encompasses the correlation of redundant, transient or implied service alarm event notifications with a specific “root cause” service alarm event notification and associated service alarm event record. <A13>

The Survey & Analyze Service Problem processes might trigger a well-defined action based on specific service alarm event notification information <A14> as well as the non-arrival of service alarm event notification information after a specific time interval has elapsed.

These processes are also responsible for monitoring and triggering the appropriate action when a service alarm event record is not cleared within a pre-defined period of time.

CENX Compliance

CENX’s Real-time Troubleshooting Module along with its Service Information Module (SIM), Northbound Interface, and Network Analytics provide the functionality necessary to monitor service alarm event notifications and manage service alarm event records in real-time.

As described in Section 2.5.1 of the CENX Product Description (A1)

With CENX Real-time Troubleshooting, network operations teams can view correlated alarms and events to Sectionalize faults, all within a single system.

CENX Monitoring and Real-time Troubleshooting:

- *gathers and displays network alarms and monitoring data from network devices and third-party applications*
- *applies fault correlation logic to determine and display the root cause fault and associated dependencies*
- *applies the alarm and fault correlation data to the visualization of the audited and verified network*
- *integrates with third-party systems to streamline workflow processes*

- Alarms are detected and Alarm Event Notifications are collected as described in Section 2.3 of the CENX Product Description (A2/A10)

Alarms and Events

CENX uses alarms and events to distinguish between incoming third-party alarm data and correlated network element events and monitoring states.

Alarms show the near real-time and historical alarm details collected from third-party systems or network elements. All available alarms are gathered and mapped to the relevant port, service segment, or network object and listed in the Alarms table for each

service. All active network alarms are listed in the Alarms table of the Monitoring Dashboard and can be refined according to Search results.

Events list the history of state changes resulting from the correlation of active alarms to network layout for each network object.

Alarms may be initialized within CENX through the Network Analytics Module. When a performance metric crosses a configured threshold and exception is initiated in an analytics report and a subsequent event/alarm is generated as described in Section 2.5 of the CENX Product Description (fulfilling **A3**)

CENX gathers port and service network statistics and utilization and performance data from network devices and third-party applications. CENX analytics consolidates and applies the information to the network inventory visualization. The performance and utilization data are tracked against predefined thresholds and CENX lists the exceptions in the analytics Reports.

When an alarm event is received it is correlated against a fault tree to determine if it is a new, related (sympathetic) or other alarm type. It is correlated against the network equipment that generated the alert which is mapped to service, physical, and location topologies – (fulfilling **A4/A5**)

Chapter 3 of CENX 6.1 Core Users Guide.pdf

End-to-end network and service visualization gives a geographic perspective to the network structure and state. A geographic view can suggest possible outage scenarios, suggest terrain-based equipment considerations when dispatching a technician, assist in determining the location of a reported issue, or indicate other geographic characteristics associated with the network.

Regular data collection from inventory databases and configuration and topology files ensures the ongoing accuracy in the network presentation.

Chapter 8 - Events list the history of state changes resulting from the correlation of active alarms to network layout for each network object.

The CENX Real-time Troubleshooting module receives alarms and events from the network, correlates the event to the topology within the CENX SIM and against the current fault tree to determine related alarm. The alarm is managed and classified as primary or sympathetic if another alarm is the primary to the fault. **<A8/A9/A10/A13>**

When the alarm is qualified, CENX publishes an event on the JMS northbound interface to notify external applications and to allow for a trouble ticket to be created or updated in case the alarm has been updated or the state has changed. **<A6>** A typical consumer of this event is the Track & Manage Service Problem process. The northbound event may also be received by the CENX Workflow module to orchestrate a process to correlate the event which may include an ordered process of automated and manual tasks, which may involve additional tests, retrieving further information for the event (such as estimated duration) as well as posting the result to other applications such as the Track & Manage Service Problem process. **<A14>**

The alarm is correlated against the services that are impacted by the alarm and the monitored state of the service is changed to warning or failure depending on the impact of this problem.

With each service managed within CENX, the customer owning/related to this service is known as shown in screenshot reference (Section 4.6.1 –shot 1). As described in the Service Trouble Report Section the information related to the alarm including the service and the customers are published to the problem handling process. <A11>.

CENX will generally understand the customer and their services and the relation of those services to the network. CENX does not generally understand the application for which the service is delivered. This information can be configured as a service attribute and subsequently made available for visualization and reporting. <M1>

4.1.4.1 *Level 4: 1.4.6.7.1 – Manage Service Alarm Event Notifications*

LEVEL 4 PROCESS MAPPING DETAILS 1.4.6.7.1 – Manage Service Alarm Event Notifications
<p>Brief Description:</p> <p>This process may determine that a service alarm event notification may represent a customer impacting condition. <A1> In these circumstances this process is responsible for indicating a potential customer problem to the Problem Handling processes. <A2> As a part of this indication this process is responsible for identifying the impacted deployed product instances associated with the service instances <M1> presenting alarm event notifications and passing this information to the Problem Handling processes. <A3></p>
<p>Extended Description:</p> <p>Not used for this process element</p>
<p>CENX Compliance:</p> <p>When an alarm is received it is qualified and the impacts to the customer’s services are assessed as described in Section 4.6.7 - A8/A9/A10 This if further shown from the screen shot #3 in (eTOM 4-6 Service Problem - CENX Conformance - supporting Screen Shots.pdf), The VPN service is shown along with its path and many alarms are associated to this service. However, the alarms are not classified as major impact, and therefore the customer service monitoring state remains in a ‘warning’ state, not as errored. <A1></p> <p>If the alarm is determined as a service problem, the process description in 4.6.1 describes the service problem handling process. As part of this process, the service in the CENX portal will show a monitoring state as ‘Failure’ with a colour of red. With either classification, when the</p>

state changes for the service, a northbound event is generated and optionally orchestrated using the CENX Workflow module. <A2>

The service identified is tied to a customer as shown in reference document screenshots (SS 4.6.1-#1).

Generally, CENX does not track the applications for which the services are delivered. However, the product reference can be configured as service attributes and made available as part of the notification process. <M1>

As described in 4.6.1, for each service event identified, CENX will correlate the event, identifying the trouble and initiate service problem management processes to resolve it. As can be seen in supporting screen shot #1 for this Section, BMC Remedy tickets have been created and referenced to the issue. The ticket is created with the source of the problem, the set of services impacted by the trouble and other supplemental information. Clicking on the trouble from the CENX portal would bring you to the external Problem Management application. <A3>

4.1.4.2 *Level 4: 1.4.6.7.2 – Record Service Performance Quality Data*

LEVEL 4 PROCESS MAPPING DETAILS 1.4.6.7.2 – Record Service Performance Quality Data	
Brief Description:	This process assesses and records received specific service performance quality data which is within tolerance limits for performance quality standards, and for which continuous monitoring and measuring of performance is required. It records the results of the continuous monitoring for reporting through the Report Service Quality Performance processes, and logs specific service performance quality degradation and violation details within the repository in the Manage Service Inventory processes to ensure historical records are available to support the needs of other processes. <A>
Extended Description:	Not used for this process element
CENX Compliance:	CENX has the ability to ingest a variety of Service Performance Quality Data, associate the data against the services related to that data, present the data to the users and perform various analytics based on this data. CENX Analytics modules as described in the Product Description Section 2.6 perform these functions. Sample screenshots representing performance quality data are provided in the screenshot document Section 4.6.7. Additional CENX Product modules perform specific business functions from the service performance data including the SLA

Management module (Product Description Section 2.7), and the Capacity Planning module (Product Description Section 2.8).

4.1.4.3 *Level 4: 1.4.6.7.3 – Correlate Service Alarm Event Notifications*

LEVEL 4 PROCESS MAPPING DETAILS	
1.4.6.7.3 – Correlate Service Alarm Event Notifications	
Brief Description:	This process encompasses the correlation of redundant, transient or implied service alarm event notifications with a specific “root cause” service alarm event notification and associated service alarm event record. This process correlates service alarm event notifications to planned outage notifications to remove false service alarm event notifications arising as a result of the planned outage activity.<A>
Extended Description:	Not used for this process element
CENX Compliance:	<p>When an alarm event is received it is correlated against a fault tree to determine if it is a new, related (sympathetic) or other alarm type. It is correlated with the network equipment that generated the alert, which is mapped to service, physical and location topologies)</p> <p><i>Chapter 3 of CENX 6.1 Core Users Guide.pdf</i></p> <p><i>End-to-end network and service visualization gives a geographic perspective to the network structure and state. A geographic view can suggest possible outage scenarios, suggest terrain-based equipment considerations when dispatching a technician, assist in determining the location of a reported issue, or indicate other geographic characteristics associated with the network.</i></p> <p><i>Regular data collection from inventory databases and configuration and topology files ensures the ongoing accuracy in the network presentation.</i></p> <p><i>Chapter 8 - Events list the history of state changes resulting from the correlation of active alarms to network layout for each network object.</i></p>

4.1.4.4 *Level 4: 1.4.6.7.4 - Abate Service Alarm Event Records*

LEVEL 4 PROCESS MAPPING DETAILS 1.4.6.7.4 - Abate Service Alarm Event Records	
Brief Description:	This process includes the notification of new service alarm event records, or status changes of previously reported service alarm event records, as well as abatement messages when service alarm event records have been cleared. <A>
Extended Description:	Not used for this process element
CENX Compliance:	Service alarm event notification analysis encompasses the identification of the service alarm event in terms of reporting entity and nature of the service alarm event. CENX will then analyze the service alarm events based on a number of criteria and then suppress redundant, transient or implied service alarm events by means of filtering and correlation, This process includes the notification of new service alarm event records, or status changes of previously reported service alarm event records, as well as abatement messages when service alarm event records have been cleared.

4.1.4.5 *Level 4: 1.4.6.7.5 - Trigger Defined Service Alarm Action*

LEVEL 4 PROCESS MAPPING DETAILS 1.4.6.7.5 - Trigger Defined Service Alarm Action
<p>Brief Description:</p> <p>This process triggers a well-defined action based on specific service alarm event notification information as well as the non-arrival of service alarm event notification information after a specific time interval has elapsed. <A> This process is also responsible for monitoring and triggering the appropriate action when a service alarm event record is not cleared within a pre-defined period of time.<AM></p>
<p>Extended Description:</p> <p>Not used for this process element</p>
<p>CENX Compliance:</p> <p>When the alarm is qualified, CENX publishes an event on the JMS northbound interface to notify external applications and to allow for a trouble ticket to be created or updated in case the alarm has been updated or the state has changed. (as described in Product Description Section 2.5.8). A typical consumer of this event is the Track & Manage Service Problem process. The northbound event may also be received by the CENX Workflow module to orchestrate a process to coordinate the event which may include an ordered process of automated and manual tasks, additional tests, retrieving further information for the event (such as estimated duration) and posting the result to other applications such as the Track & Manage Service Problem process.</p> <p>CENX workflow manager can also receive the alarms, alarm state changes, and state alarm and execute a BPMN business process, notifying appropriate users or applications and orchestrating a process to escalate the resolution of the issue.</p> <p>CENX records the state transitions and the time these occur. When an alarm is not cleared has not been cleared within a pre-defined period of time the CENX analytics and reporting framework can be readily configured to trigger a subsequent 'stale alarm' event and notify appropriate applications through the north bound interface (Product Description 2.5.8 – Originated Alarm Messages).</p>

4.1.4.6 *Level 4: 1.4.6.7.6 – Monitor Service Alarms Events*

LEVEL 4 PROCESS MAPPING DETAILS 1.4.6.7.6 - Monitor Service Alarms Events
Brief Description: This process is responsible for collecting and monitoring events and alarms provided by services through systems and monitoring tools.<A>
Extended Description: Not used for this process element
CENX Compliance: CENX’s Real-time Troubleshooting module along with its Service Information Model (SIM), Northbound Interface, and Network Analytics provide the functionality necessary to monitor service alarm event notifications and manage service alarm event records in real-time. As described in Section 2.5.1 of the CENX Service Intelligence Product Description (A) <i>With CENX Real-time Troubleshooting, network operations teams can view correlated alarms and events to Sectionalize faults, all within a single system. CENX Monitoring and Real-time Troubleshooting:</i> <ul style="list-style-type: none">• <i>gathers and displays network alarms and monitoring data from network devices and third-party applications</i>• <i>applies fault correlation logic to determine and display the root cause fault and associated dependencies</i>• <i>applies the alarm and fault correlation data to the visualization of the audited and verified network</i>• <i>integrates with third-party systems to streamline workflow processes</i>

4.1.4.7 *Level 4: 1.4.6.7.7 – Categorize Service Alarm Event*

LEVEL 4 PROCESS MAPPING DETAILS 1.4.6.7.7 - Categorize Service Alarm Event
Brief Description: This process is responsible for categorizing the service alarm events in order to support the management, filtering and correlation of events at SM&O level.<A>
Extended Description: Not used for this process element
CENX Compliance: CENX’s Real-time Troubleshooting module along with its Service Information Model (SIM), Northbound Interface, and Network Analytics provide the functionality necessary to monitor service alarm event notifications and manage service alarm event records in real-time. As described in Section 2.5.1 of the CENX Product Description (A) <i>With CENX Real-time Troubleshooting, network operations teams can view correlated alarms and events to Sectionalize faults, all within a single system. CENX Monitoring and Real-time Troubleshooting:</i> <ul style="list-style-type: none">• <i>gathers and displays network alarms and monitoring data from network devices and third-party applications</i>• <i>applies fault correlation logic to determine and display the root cause fault and associated dependencies</i>• <i>applies the alarm and fault correlation data to the visualization of the audited and verified network</i>• <i>integrates with third-party systems to streamline workflow processes</i> When an alarm event is received it is correlated against a fault tree to determine if it is a new, related (sympathetic) or other alarm type. It is correlated against the network equipment which generated the alert which is mapped to service, physical and location topologies. <i>Chapter 3 of CENX 6.1 Core Users Guide.pdf</i> <i>End-to-end network and service visualization gives a geographic perspective to the network structure and state. A geographic view can suggest possible outage scenarios, suggest terrain-based equipment considerations when dispatching a technician, assist in determining the location of a reported issue, or indicate other geographic characteristics associated with the network.</i>

Regular data collection from inventory databases and configuration and topology files ensures the ongoing accuracy in the network presentation.

Chapter 8 - Events list the history of state changes resulting from the correlation of active alarms to network layout for each network object.

The CENX Real-time Troubleshooting module receives alarms and events from the network, correlates the event to the topology within the CENX SIM and against the current fault tree to determine related alarm. The alarm is managed and classified as primary or sympathetic if another alarm is the primary to the fault. The Customer services that are served by the impacted resources, associated to the alarm, are identified and used to further classify the priority of the alarm based on the number of customer services impacted. This can be seen in the supporting screenshots document (Section 4.6.1 – Service Trouble Report) where a list of alarms impacting the subscriber’s services are displayed and the ‘service impacted’ count is linked to each alarm.

4.1.5 Supporting Evidence References

- Exanova_6.1_Service Intelligence Product Description.pdf
- cenx_exanova_6.1_core_users_guide.pdf
- eTOM 4-6 Service Problem - CENX Conformance - supporting Screen Shots.pdf

4.1.6 Level 4/Level 3 Detailed Scores

Table 4-1 1.4.6 Service Problem Management – Level 4 & Level 3 Scores

CENX V6.1	
Framework 16.0 Business Process Framework Conformance Scores	
1.4 Service Domain	
Level 2: 1.4.6 - Service Problem Management	Conformance
1.4.6.1 - Create Service Trouble Report	4.5
1.4.6.1.1 – Generate Service Problem	100%
1.4.6.1.2 – Convert Report to Service Problem Format	100%
1.4.6.1.3 – Estimate Time for Restoring Service	25%
1.4.6.2 - Diagnose Service Problem	5
1.4.6.2.1 – Verify Service Configuration	100%
1.4.6.2.2 – Perform Specific Service Problem Diagnostics	100%
<i>1.4.6.3 - Correct & Resolve Service Problem</i>	<i>Not in Scope</i>
<i>1.4.6.4 - Track & Manage Service Problem</i>	<i>Not in Scope</i>
<i>1.4.6.5 - Report Service Problem</i>	<i>Not in Scope</i>
1.4.6.6 - Close Service Trouble Report	5
1.4.6.7 - Survey & Analyze Service Problem	4.8
1.4.6.7.1 – Manage Service Alarm Event Notifications	50%
1.4.6.7.2 – Record Service Performance Quality Data	100%
1.4.6.7.3 – Correlate Service Alarm Event Notifications	100%
1.4.6.7.4 - Abate Service Alarm Event Records	100%
1.4.6.7.5 - Trigger Defined Service Alarm Action	75%
1.4.6.7.6 - Monitor Service Alarms Events	100%
1.4.6.7.7 - Categorize Service Alarm Event	100%
<i>1.1.1.10.3 - Produce & Distribute Bill</i>	<i>Not in Scope</i>

4.2 Level 2: 1.4.7 - Service Quality Management

4.2.1 Level 3: 1.4.7.1 – Monitor Service Quality

LEVEL 3 PROCESS MAPPING DETAILS 1.4.7.1 – Monitor Service Quality
Brief Description: Monitor received service quality information and undertake first-in detection.
Extended Description: The objective of the Monitor Service Quality processes is to monitor received service quality information and undertake first-in detection. The responsibilities of the processes include, but are not limited to: <ul style="list-style-type: none">• Undertake the role of first in detection and collection by monitoring and logging the received specific service performance quality data• Comparing the received specific service performance quality data to performance quality standards set for each specific service (available from the Service Inventory);• Assessing and recording received specific service performance quality data which is within tolerance limits for performance quality standards, and for which continuous monitoring and measuring of performance is required;• Recording the results of the continuous monitoring for reporting through the Report Service Quality Performance processes;• Detect performance quality threshold violations which represent specific service failures due to abnormal performance;• Pass information about specific service failures due to performance quality threshold violations to Service Problem Management to manage any necessary restoration activity as determined by that process;• Pass information about potential specific customer SLA/QoS performance degradations arising from specific service quality performance degradations (using knowledge about service to purchased product offering linkages) to Problem Handling to manage any necessary restoration activity as determined by that process;• Detect performance degradation for specific services which provide early warning of potential issues;• Forward service performance degradation notifications to other Service Quality Management processes, which manage activities to restore normal specific service

performance quality

- Log specific service performance quality degradation and violation details within the repository in the Manage Service Inventory processes to ensure historical records are available to support the needs of other processes.

The processes also perform automated service testing using simulated calls simulating standard user behavior, and collect data related to service usage which may supply information to other processes (i.e. marketing, service cost, etc.) and identify abnormal usage by the service users (i.e. bad passwords, terminal configurations, etc.).

CENX Compliance

(L3 process with L4 Definitions – see L4 Responses)

4.2.1.1 *Level 4: 1.4.7.1.1 – Manage Service Performance Quality Data*

LEVEL 4 PROCESS MAPPING DETAILS

1.4.7.1.1 – Manage Service Performance Quality Data

Brief Description:

This process monitors and logs the received specific service performance quality data, <A1>

compares the received specific service performance quality data to performance quality standards set for each specific service (available from the Service Inventory) <A2>

detect performance quality threshold violations which represent specific service failures due to abnormal performance, and detects performance degradation for specific services which provide early warning of potential issues. <A3>

Extended Description:

CENX Compliance

CENX derives a service and resource topology dynamically based on collected and analyzed data from the network and from a variety of operational database applications such as Resource Inventory, Service Inventory, and Customer Relationship Management (CRM) software to establish a validated, audited model of network inventory.

Service and network performance and utilization data is then collected from a variety of testing and monitoring applications, and managed within the CENX platform. The data is presented in context as part of the CENX Operations console associated to the relevant network elements and impacted services and analyzed for fault detection, SLA violations, performance degradation and a variety of other reporting platforms.

The CENX 6.1 Product Description describes the ingestion of various performance data such as TWAMP and ITU testing data in Section 2.6.2. Section 2.6.3 shows further detail including screenshots showing the test data available for the given service. Screen shots from the application are also provided

- Section 1.1.1 shows the CENX portal with a service view with all the resources delivering the service. Selecting one of the graph icons on any of the involved resources will show the available performance and utilization data at the appropriate measurement point in the service path.
- Section 1.1.2 shows results during a time of failure, where performance data is measured at various points on the service path. Analyzing the data allows the performance problem to be isolated to an appropriate part of the network. In this example Frame Delay information is analyzed and presented. Once can see that the analysis isolated the violating segment to a RAN network segment, marked the service as impaired and highlighted the impaired segment.

Threshold Crossing Alerts (TCA) are supported in the platform as described in Product Description Section 2.6.1. TCA compares the received specific service performance quality data to performance quality standards set for each specific service (available from the CENX Service Information Model - SIM). In this scenario, CENX monitors performance and utilization data for each service and data set and generates alarms for the given service based on a configured performance level threshold.

Further evidence for TCA is provided in Screen Shots Reference Section 1.1.3. In this example, Frame Loss is over the configured service quality standard of 3.33% and an alarm is generated showing the service with jeopardy status. <A2/A3>

4.2.1.2 *Level 4: 1.4.7.1.2 – Record Service Performance Quality Data*

LEVEL 4 PROCESS MAPPING DETAILS 1.4.7.1.2 – Record Service Performance Quality Data
<p>Brief Description:</p> <p>This process assesses and records received specific service performance quality data which is within tolerance limits for performance quality standards, and for which continuous monitoring and measuring of performance is required. <A1> It records the results of the continuous monitoring for reporting through the Report Service Quality Performance processes, and logs specific service performance quality degradation and violation details within the repository in the Manage Service Inventory processes to ensure historical records are available to support the needs of other processes. <A2></p>
<p>Extended Description:</p>
<p>CENX Compliance</p> <p>The CENX Product Description describes the ingestion of various performance data such as TWAMP and ITU testing data in our response for 4.7.1.1.</p> <p>As described above, CENX assesses the performance quality data and measures it to be within tolerance limits through the Threshold Crossing Alert (TCA) framework as described in Product Description Section 2.6.1 and further evidenced with screenshots in Section 1.1.3. <A1></p> <p>The service performance quality data is logged in the platform for further analysis. The data is available through with historic date range selection as shown in the Service view as shown in the screenshots provided (1.1.2). Further, the data is available for analytics reports and dashboarding as shown in the Product Description Section 2.6.4.3 showing Performance Reports by date range and Section 2.7.1 where SLA Violations reports are available in rollups of Daily, weekly, 7 day and monthly reports. <A2></p>

4.2.1.3 *Level 4: 1.4.7.1.3 – Correlate Service Performance Event Notifications*

LEVEL 4 PROCESS MAPPING DETAILS 1.4.7.1.3 – Correlate Service Performance Event Notifications
<p>Brief Description:</p> <p>This process passes information about specific service failures due to performance quality threshold violations to Service Problem Management to manage any necessary restoration activity as determined by that process. <A1> It passes information about potential specific customer SLA/QoS performance degradations arising from specific service quality performance degradations (using knowledge about service to purchased product offering linkages) to Problem Handling to manage any necessary restoration activity as determined by that process. <A2> It forwards service performance degradation notifications to other Service Quality Management processes, which manage activities to restore normal specific service performance quality. <A3></p> <p>Perform automated service testing using simulated calls simulating standard user behavior, collect data related to service usage <A4></p>
<p>Extended Description:</p>
<p>CENX Compliance</p> <p>When CENX detects a threshold-crossing event (aka Performance Quality Threshold Violation), the Analytics module will generate an appropriate alert for this type of event. In the case of quality impairment, an alarm is generated and passed to Northbound Interface (for consumption by external applications) and processed by the CENX Real-time Troubleshooting module to manage as an alarm for that service. Once the Real-time Troubleshooting module validates the alarm and determines the impacted services, it generates additional Northbound alert messages, decorated with alarm information and additional information about each impacted service. This process is described in Product Description Section 2.6.1 (Threshold Crossing Alerts), Section 2.5.8 (Northbound Interface) and Section 2.5.1 (Real-time Troubleshooting). Screen shot 1.1.3 shows a TCA violation and the corresponding alarms that were generated, and visibility of those alarms to the impacted service. <A1></p> <p>Alerts to external Problem Handling processes are supported through the above process:</p> <ul style="list-style-type: none">- The performance data analytics module will detect threshold violations or other rule violations and generate an alert available to northbound applications, with information about the local test data being used.- The Real-time Troubleshooting module will validate the alerts, possibly determine the alert is primary or secondary to a given problem, identify all impacted services and generate a notification for external applications with the service details. Generally CENX

will maintain reference to the CFS and RFS service information associated to a customer and the corresponding service address. This information is all available for notification to northbound applications. <A2/A3>

- If additional workflow processes are required for alarm processing the CENX workflow manager can be readily configured for further business processing including decorating the alarms with customer product information by querying an external customer product information data store.

Generally service quality performance tests are run on a scheduled basis and collected and subsequently managed by CENX as the test results are available. Additional tests can be triggered by the users to be run on-demand tests as shown in Screen shot Section 4.7.1 – ‘Run Tests’ – selecting this link will initiate a service level test and present the results. <A4>

4.2.1.4 *Level 4: 1.4.7.2 – Analyze Service Quality*

LEVEL 4 PROCESS MAPPING DETAILS

1.4.7.2 – Analyze Service Quality

Brief Description:

Analyze and evaluate the service quality performance of specific services.

Extended Description:

The purpose of the Analyze Service Quality processes is to analyze the information received from the Monitor Service Quality process to evaluate the service quality performance of specific services.

Using the data from Monitor Service Quality, these processes will correlate events in order to filter repetitive alarms and failure events that do not affect the quality delivered, and they will calculate key service quality indicators, (such as Mean Time Between Failures and other chronic problems).

The responsibilities of the processes include, but are not limited to:

- Undertaking analysis as required on specific service performance information received from the Monitor Service Quality processes;
- Initiating, modifying and cancelling continuous performance data collection schedules for specific services required to analyze specific service performance. These schedules are established through requests sent to the Enable Service Quality Management processes.
- Determining the root causes of specific service performance degradations and violations;
- Recording the results of the analysis and intermediate updates in the Service Inventory

<p>for historical analysis and for use as required by other processes</p> <ul style="list-style-type: none"> • Undertaking specific detailed analysis (if the original requested came from Customer QoS/SLA Management processes) to discover the root cause of customer QoS performance degradations that may be arising due to interactions between service instances, without any specific service instance having an unacceptable performance in its own right..
<p>CENX Compliance (L3 process with L4 Definitions – see L4 Responses)</p>

4.2.1.5 *Level 4: 1.4.7.2.1 – Perform Specific Service Performance Diagnostics*

<p>LEVEL 4 PROCESS MAPPING DETAILS 1.4.7.2.1 – Perform Specific Service Performance Diagnostics</p>
<p>Brief Description:</p> <p>This process performs analysis as required on specific service performance information received from the Monitor Service Quality processes. It determines the root causes of specific service performance degradations and violations, <A1> records the results of the analysis <A2> and intermediate updates in the Service Inventory for historical analysis and for use as required by other processes, <A3> and undertakes specific detailed analysis (if the original requested came from Customer QoS/SLA Management processes) to discover the root cause of customer QoS performance degradations that may be arising due to interactions between service instances, without any specific service instance having an unacceptable performance in its own right.<A4></p>
<p>Extended Description:</p>
<p>CENX Compliance</p> <p>The CENX Real-time Troubleshooting module is the primary component to performance specific service diagnostics. As described in Monitor Service Quality, CENX ingests, manages, monitors and analyzes performance data and generates alerts for various violations. The CENX Real-time Troubleshooting Module will accept these alerts, and determine the priority of the alert, qualify the alert as primary or sympathetic and report on the issue.</p> <p>The root cause processing is described in the Product Description Section 2.5.1 where fault correlation logic is executed to determine the root cause of the alert. <A1></p> <p>The results of the analysis are reported on the network elements and the impacted services related to the alarm. The performance data is available as shown in supporting screenshots Section 1.1.2 and the service status is shown the same screen shot with a status of 'ok',</p>

'warning', 'dependency' or 'failed'. The resulting alarms are displayed with the service as shown in screen shot 1.1.3 <A2>

The results of the enriched alarm and the subsequent processing are published through the Northbound Interface as described in Product Description Section 2.5.8. <A3>

Threshold Crossing Alerts (TCAs) may be generated for varying levels of metrics, and problems can be detected and ideally resolved before service impairment is realized by the customer.

TCAs can be generated when the service metrics are approaching a SLA violation (such as 75% of threshold) or are trending in a negative direction (10% over historic average). These proactive alerts are classifying as alerts rather than alarms in the TCA configuration, alerts are published and received by the Real-time Troubleshooting module which may classify the service with a 'warning' status and trigger notifications to northbound applications for proactive resolution. <A4>

4.2.1.6 *Level 4: 1.4.7.2.2 - Manage Service Performance Data Collection Schedules*

LEVEL 4 PROCESS MAPPING DETAILS

1.4.7.2.2 – Manage Service Performance Data Collection Schedules

Brief Description:

This process initiates, modifies and cancels continuous performance data collection schedules for specific services required to analyze specific service performance. These schedules are established through requests sent to the Enable Service Quality Management processes. <A>

Mandatory:

This process initiates, modifies and cancels continuous performance data collection schedules for specific services required to analyze specific service performance.

CENX Compliance

CENX maintains a current inventory of all services and the path of resources involved to deliver that service. This inventory is maintained in the CENX Service Information Model (SIM) as described in Product Description Section 2.2.

The SIM is established by ingesting data from a variety of sources including live network configuration data, coupled with inventory data from BSS and OSS applications as described in the Continuous Data Ingest, Audit and Integrity Section of the Product Description (Section 2.3).

As services are discovered through this process, CENX generates an event that can initiate a BPMN process, which will orchestrate the publication of this service to external applications including the 'Enable Service Quality Management' process. Similarly as these services are changed or removed distinct BPMN processes can be triggered. This workflow capability is described in the Product Description Section 2.9 and specifically for service detection in Section 2.9.4.

4.2.2 Level 3: 1.4.7.5 – Create Service Performance Degradation Report

LEVEL 3 PROCESS MAPPING DETAILS 1.4.7.5 – Create Service Performance Degradation Report
Brief Description: Create a new service performance degradation report.
Extended Description: <p>The objective of the Create Service Performance Degradation Report process is to create a new service performance degradation report, modify existing service performance degradation reports, and request cancellation of existing service performance degradation reports.</p> <p>A new service performance degradation report may be created as a result of specific service performance notifications undertaken by the Monitor Service Performance processes, or at the request of analysis undertaken by other CRM, SM&O or RM&O processes which detect that some form of deterioration or failure has occurred requires an assessment of the specific service performance.</p> <p>If the service performance degradation report is created as a result of a notification or request from processes other than Monitor Service Performance processes, the Create Service Performance Degradation Report processes are responsible for converting the received information into a form suitable for the Service Performance Management processes, and for requesting additional information if required.</p>
CENX Compliance (L3 process with L4 Definitions – see L4 Responses)

4.2.2.1 *Level 4: 1.4.7.5.1 – Generate Service Performance Degradation Problem*

LEVEL 4 PROCESS MAPPING DETAILS 1.4.7.5.1 – Generate Service Performance Degradation Problem
Brief Description: <p>This process creates a new Service Performance Degradation Report as a result of specific service performance notifications undertaken by the Monitor Service Performance processes, or at the request of analysis undertaken by other CRM, SM&O or RM&O processes which detect that some form of deterioration or failure has occurred requires an assessment of the specific service performance. <A></p>
Mandatory:
CENX Compliance <p>CENX’s Analytics module manages performance data and initiates an alert when a threshold has been met. This threshold may be a service SLA violation or it may be configured as a warning such as when the service performance is degrading or approaching an SLA violation (e.g. 80% of SLA). The threshold will generate an alert which is published through the North Bound Interface for consumption by interested applications and by the CENX Real-time Troubleshooting Module.</p> <p>As described in this paper, Section 4.7.2.1 – the Real-time Troubleshooting module will accept this performance degradation alert, and perform root cause analysis in a manner consistent with alarm processing. The service is marked with a status of ‘warning’, the service and impacted resource elements are marked in a ‘warning’ in the CENX Portal and a notification is generated on the Northbound interface (Product Description Section 2.5.8) highlighting the warning. All alarms and alerts are displayed in this CENX Portal as shown in Supporting Screen Shots Section 1.1.3.</p>

4.2.2.2 *Level 4: 1.4.7.5.2 – Convert Report To Service Performance Degradation Report Format*

LEVEL 4 PROCESS MAPPING DETAILS 1.4.7.5.2 – Convert Report To Service Performance Degradation Report Format
<p>Brief Description:</p> <p>If the service performance degradation report is created as a result of a notification or request from processes other than Monitor Service Performance processes, this process responsible for converting the received information into a form suitable for the Service Performance Management processes, and for requesting additional information if required. <A></p>
<p>Mandatory:</p> <p>This process is responsible for converting the received information into a form suitable for the Service Performance Management processes, and for requesting additional information if required.</p>
<p>CENX Compliance</p> <p>CENX detects notifications to external applications for the Service Performance Degradation through the NorthBound Interface as described in the Product Description Section 2.5.8.</p> <p>The Service Performance Degradation Report may be further extended with more information by executing a business process as described in the workflow manager Section 2.9.4</p> <p>Reports showing all active alarms or alerts (see TCA Events) are also visible and exportable for other applications as can be seen in the supporting Screen Shot document Section 4.7.5.</p>

4.2.3 Level 3: 1.4.7.7 – Close Service Performance Degradation Report

LEVEL 3 PROCESS MAPPING DETAILS 1.4.7.7 – Close Service Performance Degradation Report
<p>Brief Description:</p> <p>Close a service performance degradation report when the service performance has been resolved <A></p>
<p>Extended Description:</p> <p>The objective of the Close Service Performance Degradation Report processes is to close a service performance degradation report when the service performance has been resolved. These processes monitor the status of all open service performance degradation reports, and recognize that a service performance degradation report is ready to be closed when the status is changed to cleared.</p>
<p>CENX Compliance</p> <p>CENX Real-time Troubleshooting manages each alarm and alert with a status that needs to be updated. As CENX Analytic detects that the performance degradation no longer exists it will generate a cancel alert message. This message is published by the Northbound interface for external applications and processed by the CENX Real-time Troubleshooting module. The Troubleshooting module will update the current service updating the service to an appropriate monitoring status (status:OK/green if no other alerts/alarms). The events are all maintained in the CENX datastore for future analysis.</p> <p>Screen shots – 4.7.5 shows the performance report being a list of alarms, one can see TCA raised at the bottom of the list showing a warning and a TCA cleared when the performance degradation issue is resolved.</p>

4.2.4 Supporting Evidence References

- Exanova_6.1_Service Intelligence Product Description.pdf
- eTOM 4-7 Service Quality - CENX Conformance - supporting Screen Shots v0-1

4.2.5 Level 4/Level 3 Detailed Scores

Table 4-2 1.4.7 Service Quality Management – Level 4 & Level 3 Scores

CENX V6.1 Framework 16.0 Business Process Framework Conformance Scores	
1.4 Service Domain	
Level 2: 1.4.7 - Service Quality Management	Conformance
1.4.7.1 - Monitor Service Quality	5
1.4.7.1.1 – Manage Service Performance Quality Data	100%
1.4.7.1.2 – Record Service Performance Quality Data	100%
1.4.7.1.3 – Correlate Service Performance Event Notifications	100%
1.4.7.2 - Analyze Service Quality	5
1.4.7.2.1 – Perform Specific Service Performance Diagnostics	100%
1.4.7.2.2 – Manage Service Performance Data Collection	100%
<i>1.4.7.3 - Improve Service Quality</i>	<i>Not in Scope</i>
<i>1.4.7.4 - Report Service Quality Performance</i>	<i>Not in Scope</i>
1.4.7.5 - Create Service Performance Degradation Report	5
1.4.7.5.1 – Generate Service Performance Degradation	100%
1.4.7.5.2 – Convert Report To Service Performance	100%
<i>1.4.7.6 - Track & Manage Service Quality Performance Resolution</i>	<i>Not in Scope</i>
1.4.7.7 - Close Service Performance Degradation Report	5

4.3 Level 2: 1.5.8 – Resource Trouble Management

4.3.1 Level 3: 1.5.8.1 - Survey & Analyze Resource Trouble

LEVEL 3 PROCESS MAPPING DETAILS 1.5.8.1 - Survey & Analyze Resource Trouble
<p>Brief Description:</p> <p>Monitor resource alarm event notifications and manage resource alarm event records in real-time. Resource alarm event notifications include those alarms related to security events.</p>
<p>Extended Description:</p> <p>The objective of the Survey & Analyze Resource Trouble processes is to monitor resource alarm event notifications and manage resource alarm event records in real-time.</p> <p>Responsibilities of the Survey & Analyze Resource Trouble processes include, but are not limited to:</p> <ul style="list-style-type: none">• Detecting and collecting resource alarm event notifications;• Initiating and managing resource alarm event records;• Performing resource alarm event notification localization analysis;• Correlating and filtering resource alarm event records;• Reporting resource alarm event record status changes to other processes• Managing resource alarm event record jeopardy conditions. <p>Resource alarm event notification analysis encompasses the identification of the resource alarm event in terms of reporting entity and nature of the resource alarm event. It will then analyze the resource alarm events based on a number of criteria and then suppress redundant, transient or implied resource alarm events by means of filtering and correlation. It includes the notification of new resource alarm event records, or status changes of previously reported resource alarm event records, as well as abatement messages when resource alarm event records have been cleared.</p> <p>The analysis will correlate resource alarm event notifications to planned outage notifications to remove false resource alarm event notifications arising as a result of the planned outage activity.</p> <p>These processes may determine that a resource alarm event notification may represent a service impacting condition. In these circumstances this process is responsible for indicating a potential service problem to the Service Problem Management processes. As a part of this indication this process is responsible for identifying the impacted service instances associated with the resource instances presenting alarm event notifications and passing this information to the Service Problem Management processes.</p> <p>Resource alarm event record correlation and filtering encompasses the correlation of redundant,</p>

transient or implied resource alarm event notifications with a specific “root cause” resource alarm event notification and associated resource alarm event record.

The Survey & Analyze Resource Trouble processes might trigger a well-defined action based on specific resource alarm event notification information as well as the non-arrival of resource alarm event notification information after a specific time interval has elapsed.

These processes are also responsible for monitoring and triggering the appropriate action when a resource alarm event record is not cleared within a pre-defined period of time.

CENX Compliance

(L3 process with L4 Definitions – see L4 Responses)

4.3.1.1 *Level 4: 1.5.8.1.1 - Manage Resource Alarm Event Notifications*

LEVEL 4 PROCESS MAPPING DETAILS

1.5.8.1.1 – Manage Resource Alarm Event Notifications

Brief Description:

This process may determine that a resource alarm event notification may represent a service impacting condition <A1>. In these circumstances this process is responsible for indicating a potential service problem to the Service Problem Management processes <A2>. As a part of this indication this process is responsible for identifying the impacted service instances associated with the resource instances presenting alarm event notifications and passing this information to the Service Problem Management processes. <A3>

Extended Description:

Not used for this process element

CENX Compliance

The CENX Real-time Troubleshooting module is the primary component to manage Resource Alarm Events. As described in the Product Description (Section 2.5.1), the module receives an alarm, associate it to the appropriate network resource, performs fault correlation to classify the alarm and determines the customer service impact as a result of the alarm. (A1).

CENX will generate a northbound alert after processing this alarm as described in the Product Description Section 2.5.8. This alert can be received by an external Service Problem Management process to perform additional processing. When CENX performs the role of Service Problem Management, the notification is managed internally and logically processed as described in CENX’s response to eTOM Service Problem Management processes. Please also see screen shot 5.8.1-1 to show all resource alarms impacting a customer service and the screenshot 5.8.1-2 to show the list of services impacted by an alarm. (A2)

The customer services associated with each alarm are recognized as described in the Product Description (Section 2.5.1) and included in the NBI, visualized in the CENX portal and made available through the CENX Service Problem Management processes. (A3)

4.3.1.2 *Level 4: 1.5.8.1.2 - Filter Resource Alarm Event Notifications*

LEVEL 4 PROCESS MAPPING DETAILS	
1.5.8.1.2 – Filter Resource Alarm Event Notifications	
Brief Description:	This process encompasses the identification of the resource alarm event in terms of reporting entity and nature of the resource alarm event.<A1> It then analyzes the resource alarm events based on a number of criteria and then suppresses redundant, transient or implied resource alarm events by means of filtering and correlation<A2>
Extended Description:	Not used for this process element
CENX Compliance	<p>CENX manages the resource alarm event, maintaining the original information and enriching it with additional value-added data such as the list of impacted customer services. In the Product Description Section 2.5.4 we describe all the attributes of the alarm including the device that generated the fault, the fault type, timestamp, severity and notes to capture further details of the event. (A1).</p> <p>CENX then analyzes the alarm building a fault tree by applying fault correlation logic to determine and display the root cause fault and associated dependencies as described in the Product Description Section 2.5.1. By this method the alarms are classified by severity level, and determined as either root cause or sympathetic (alarm caused by another alarm). All alarms are presented with the classification information through the CENX portal in the service view (Screenshot 5.8.1-1) and the alarm monitoring view (Screenshot 5.8.1-3) and reported in the North-bound interface. (A2)</p>

4.3.1.3 *Level 4: 1.5.8.1.3 - Correlate Resource Alarm Event Notifications*

LEVEL 4 PROCESS MAPPING DETAILS 1.5.8.1.3 – Correlate Resource Alarm Event Notifications
<p>Brief Description:</p> <p>Resource alarm event record correlation and filtering encompasses the correlation of redundant, transient or implied resource alarm event notifications with a specific “root cause” resource alarm event notification and associated resource alarm event record. <A1> This process correlates resource alarm event notifications to planned outage notifications to remove false resource alarm event notifications arising as a result of the planned outage activity. <A2></p>
<p>Extended Description:</p> <p>Not used for this process element</p>
<p>CENX Compliance</p> <p>CENX then analyzes the alarm building a fault tree by applying fault correlation logic to determine and display the root cause fault and associated dependencies as described in the Product Description Section 2.5.1. By this method the alarms are classified by severity level, and determined as root cause or sympathetic (alarm caused by another alarm).</p> <p>When an alarm event is received it is correlated against a fault tree to determine if it is a new, related (sympathetic) or other alarm type. It is correlated against the network equipment which generated the alert which is mapped to service, physical and location topologies)</p> <p>Chapter 3 of CENX 6.1 Core Users Guide.pdf</p> <p>End-to-end network and service visualization gives a geographic perspective to the network structure and state. A geographic view can suggest possible outage scenarios, suggest terrain-based equipment considerations when dispatching a technician, assist in determining the location of a reported issue, or indicate other geographic characteristics associated with the network.</p> <p>Regular data collection from inventory databases and configuration and topology files ensures the ongoing accuracy in the network presentation.</p> <p>Chapter 8 - Events list the history of state changes resulting from the correlation of active alarms to network layout for each network object.</p>

4.3.1.4 *Level 4: 1.5.8.1.4 - Abate Alarm Event Records*

<p style="text-align: center;">LEVEL 4 PROCESS MAPPING DETAILS 1.5.8.1.4 – Abate Alarm Event Records</p>
<p>Brief Description:</p> <p>This process includes the notification of new resource alarm event records, or status changes of previously reported resource alarm event records, as well as abatement messages when resource alarm event records have been cleared.<A1></p>
<p>Extended Description:</p> <p>Not used for this process element</p>
<p>CENX Compliance</p> <p>Resource alarm event notification analysis encompasses the identification of the resource alarm event in terms of reporting entity and nature of the alarm event. CENX analyzes the alarm events based on a number of criteria and then suppress redundant, transient or implied alarm events by means of filtering and correlation It includes the notification of new alarm event records, or status changes of previously reported alarm event records, as well as abatement messages when alarm event records have been cleared.</p>

4.3.1.5 *Level 4: 1.5.8.1.5 – Trigger Defined Action*

LEVEL 4 PROCESS MAPPING DETAILS 1.5.8.1.5 – Trigger Defined Action
Brief Description: This process triggers a well-defined action based on specific resource alarm event notification information as well as the non-arrival of resource alarm event notification information after a specific time interval has elapsed. <A1> This process is also responsible for monitoring and triggering the appropriate action when a resource alarm event record is not cleared within a pre-defined period of time.<A2>
Extended Description: Not used for this process element
CENX Compliance <p>When an alarm is qualified, CENX publishes an event on the JMS Northbound interface to notify external applications and to allow for a trouble ticket to be created or updated in case the alarm has been updated or the state has changed. (as described in Product Description Section 2.5.8). A typical consumer of this event is the Track & Manage Service Problem process. The northbound event may also be received by the CENX Workflow module to orchestrate a process to coordinate the event which may include an ordered process of automated and manual tasks, which may involve additional tests, retrieving further information for the event (such as estimated duration) and post the result to other applications such as the Track & Manage Service Problem process.</p> <p>CENX workflow manager can also receive the alarms, alarm state changes, and state alarm and execute a BPMN business process, notifying appropriate users or applications and orchestrating a process to escalate the resolution of the issue. <A1></p> <p>CENX records the state transitions and the time these occur. When an alarm is not cleared has not been cleared within a pre-defined period of time the CENX analytics and reporting framework can be readily configured to trigger a subsequent 'stale alarm' event and notify appropriate applications through the north bound interface (Product Description 2.5.8 – Originated Alarm Messages). <A2></p>

4.3.1.6 *Level 4: 1.5.8.1.6 – Monitor Resource Alarms Events*

LEVEL 4 PROCESS MAPPING DETAILS 1.5.8.1.6 – Monitor Resource Alarms Events
Brief Description: This process is responsible for collecting and monitoring events and alarms provided by resources through systems and monitoring tools.
Extended Description: This process is responsible for collecting and monitoring events and alarms provided by resources through systems and monitoring tools.<A>
CENX Compliance The key module to Monitor Resource Alarm Events is the CENX Real-time Troubleshooting module along with Service Information Model (SIM), Northbound Interface, and Network Analytics. As described in Section 2.5.1 of the CENX Product Description (A) <i>With CENX Real-time Troubleshooting, network operations teams can view correlated alarms and events to Sectionalize faults, all within a single system. CENX Monitoring and Real-time Troubleshooting:</i> <ul style="list-style-type: none">• <i>gathers and displays network alarms and monitoring data from network devices and third-party applications</i>• <i>applies fault correlation logic to determine and display the root cause fault and associated dependencies</i>• <i>applies the alarm and fault correlation data to the visualization of the audited and verified network</i>• <i>integrates with third-party systems to streamline workflow processes</i>

4.3.1.7 *Level 4: 1.5.8.1.7 – Categorize Resource Alarm Event*

LEVEL 4 PROCESS MAPPING DETAILS 1.5.8.1.7 – Categorize Resource Alarm Event
Brief Description: This process is responsible for categorizing the resource alarm events in order to support the management, filtering and correlation of events at RM&O level.
Extended Description: This process is responsible for categorizing the resource alarm events in order to support the management, filtering and correlation of events at RM&O level.<A>
CENX Compliance The key module to deliver on Categorizing Resource Alarm Events is the CENX Real-time Troubleshooting module along with Service Information Model (SIM), Northbound Interface, and Network Analytics. As described in Section 2.5.1 of the CENX Product Description (A) <i>With CENX Real-time Troubleshooting, network operations teams can view correlated alarms and events to Sectionalize faults, all within a single system. CENX Monitoring and Real-time Troubleshooting:</i> <ul style="list-style-type: none">• <i>gathers and displays network alarms and monitoring data from network devices and third-party applications</i>• <i>applies fault correlation logic to determine and display the root cause fault and associated dependencies</i>• <i>applies the alarm and fault correlation data to the visualization of the audited and verified network</i>• <i>integrates with third-party systems to streamline workflow processes</i> When an alarm event is received it is correlated against a fault tree to determine if it is a new, related (sympathetic) or other alarm type. It is correlated against the network equipment which generated the alert which is mapped to service, physical and location topologies. Chapter 3 of CENX 6.1 Core Users Guide.pdf End-to-end network and service visualization gives a geographic perspective to the network structure and state. A geographic view can suggest possible outage scenarios, suggest terrain-based equipment considerations when dispatching a technician, assist in determining the location of a reported issue, or indicate other geographic characteristics associated with the network. Regular data collection from inventory databases and configuration and topology files ensures the ongoing accuracy in the network presentation.

4.3.2 Level 3: 1.5.8.2 - Localize Resource Trouble

LEVEL 3 PROCESS MAPPING DETAILS 1.5.8.2 – Localize Resource Trouble
<p>Brief Description:</p> <p>Perform analysis to identify the root cause of the specific resource trouble including those resource troubles related to security events.</p>
<p>Extended Description:</p> <p>The objective of the Localize Resource Trouble processes is to identify the root cause of the specific resource trouble. These processes are invoked by the Track & Manage Resource Trouble processes.</p> <p>The responsibilities of these processes include, but are not limited to:</p> <ul style="list-style-type: none">• Verifying whether the resource configuration matches the appropriate service features;• Performing diagnostics against the specific resources;•• Running tests against the specific resources;• Starting and stopping audits against specific resources• Scheduling routine testing of the specific resources. <p>The Localize Resource Trouble processes will make the results of the root cause analysis available to other processes. The Localize Resource Trouble processes will update the open resource trouble report, as required during the assessment, and when the root cause has been identified.</p> <p>When the process is complete the Localize Resource Trouble processes will notify the Track & Manage Resource Trouble processes.</p>
<p>CENX Compliance</p> <p>(L3 process with L4 Definitions – see L4 Responses)</p>

4.3.2.1 *Level 4: 1.5.8.2.1 - Verify Resource Configuration*

<p style="text-align: center;">LEVEL 4 PROCESS MAPPING DETAILS 1.5.8.2.1 – Verify Resource Configuration</p>
<p>Brief Description: This process verifies whether the resource configuration matches the appropriate service features. <A></p>
<p>Extended Description: Not used for this process element</p>
<p>CENX Compliance</p> <p>The CENX Continuous Data Ingest and Audit process, ingests data from the network involved in delivering a service to the customer, stitching the configurations together and comparing the results to various data sources from the BSS/OSS to ensure a complete picture of the service and resource topology is realized and that the configurations are consistent between the actual network and the desired OSS. Each topology is given a build and audit score, with the build score based on the completeness of the service and network configuration and the audit comparing the service/network configuration with that from the OSS inventories.</p> <p>The topology build is described in Product Description Section 2.2 and the process of auditing the data across data from various BSS/OSS systems is described in Section 2.3.</p>

4.3.2.2 *Level 4: 1.5.8.2.2 - Perform Specific Resource Trouble Diagnostics*

LEVEL 4 PROCESS MAPPING DETAILS	
1.5.8.2.2 – Perform Specific Resource Trouble Diagnostics	
Brief Description:	This process performs diagnostics against the specific resources. This includes application of signatures and other methods to capture anomalous events or malware. <A>
Extended Description:	Not used for this process element
CENX Compliance	<p>CENX integrates with various test probes and other test harness applications such as TWAMP, ICOMP, Performance Monitoring and Service Performance Monitoring applications as described in the Product Description Section 2.6.2. These systems generate test traffic that can be measured at various points in the network –these measurements are analyzed by CENX to perform root cause analysis and to detect and isolate a problem</p> <p>Test results from these applications are ingested into CENX and associated with the resource for which the test applies.</p> <p>The results of the tests are compared against configured metrics or threshold – when these thresholds are cross, events are triggered to process and manage the alert. The alert may be classified as an alarm and treated as defined in Survey and Analyze Service Trouble. This is described in the Product Description Section 2.6.1.</p>

4.3.2.3 *Level 4: 1.5.8.2.3 - Perform Specific Resource Trouble Tests*

LEVEL 4 PROCESS MAPPING DETAILS 1.5.8.2.3 – Perform Specific Resource Trouble Tests	
Brief Description:	This process runs tests against the specific resources. This can include penetration tests to check for vulnerabilities.<AM>
Extended Description:	Not used for this process element
CENX Compliance	CENX can be configured to accept test results from any test driver application running tests against resources that are managed in the CENX Service Information Model. The results of the tests are associated to the applicable resources, categorized and processed as defined in the Product Description Section 2.5.1.

4.3.2.4 *Level 4: 1.5.8.2.4 - Stop and Start Audit On Resources*

LEVEL 4 PROCESS MAPPING DETAILS 1.5.8.2.4 – Stop And Start Audit On Resources	
Brief Description:	This process starts and stops audits against specific resources.<A>
Extended Description:	Not used for this process element
CENX Compliance	<p>The CENX application performs a regular ingest, build and audit from a variety of data sources to build the Information Model as described in the Product Description Section 2.3.</p> <p>When new records are discovered in that build process a workflow can be triggered which can orchestrate a business process to notify various applications of the existence (or removal) of that resource. One of the steps in this process is testing applications which need to know of the creation of a new element so that tests can be performed against it. This workflow process is described in the Product Description Section 2.9.4.</p>

4.3.2.5 *Level 4: 1.5.8.2.5 - Schedule Routine Resource Trouble Tests*

LEVEL 4 PROCESS MAPPING DETAILS 1.5.8.2.5 – Schedule Routine Resource Trouble Tests	
Brief Description:	This process schedules routine testing of the specific resources including virus scans and malware testing.<A>
Extended Description:	Not used for this process element
CENX Compliance	<p>Routine tests are executed against the resources managed by CENX and the results of those tests are analyzed by the CENX Real-time Troubleshooting module (Product Description Section 2.5.1) if the test failed, or if the test data requires analytics then the results are analyzed by the</p>

Analytics module as defined in Section 2.6 of the Product Description.

The scheduling of the routine tests is performed on the discovery of new resources as described in our response in 5.8.2.4

When new records are discovered in that build process a workflow can be triggered which can orchestrate a business process to notify various applications of the existence (or removal) of that resource. One of the steps in this process is testing applications which need to know of the creation of a new element so that tests can be performed against it. This workflow process is described in the Product Description Section 2.9.4.

4.3.2.6 *Level 4: 1.5.8.2.6 – Notify T&M Root Cause Resource Trouble*

LEVEL 4 PROCESS MAPPING DETAILS

1.5.8.2.6 – Notify T&M Root Cause Resource Trouble

Brief Description:

This process makes the results of the root cause analysis available to other processes. <A1> It updates the open resource trouble report, as required during the assessment, and when the root cause has been identified <A2>. This process notifies the Track & Manage Resource Trouble processes. <A3>

Extended Description:

Not used for this process element

CENX Compliance

During the processing of a resource alarm, CENX Real time troubleshooting module will validate and classify the alarm as described in Product Description Section 2.5.1. The results of this classification is displayed in the CENX Portal and communicated to northbound application through the Northbound interface as described in Section 2.5.8. <A1>

CENX includes a Resource Trouble Report showing all resource alarms in the system and allows them to be sorted by status, impact and a variety of other fields. This report is shown in screenshots Section 5.8.1-3. <A2>

CENX will notify other applications of this event such as the Track & Manage Resource Trouble Process through the Northbound interface as described in Section 2.5.8. <A3>

4.3.2.7 *Level 4: 1.5.8.1.7 – Categorize Resource Trouble*

<p style="text-align: center;">LEVEL 4 PROCESS MAPPING DETAILS 1.5.8.1.7 – Categorize Resource Trouble</p>
<p>Brief Description:</p> <p>This process is responsible for categorizing the resource trouble according to the type of the trouble, impact, and standardized criteria at RM&O level. Moreover, this activity will be carried out with appropriate diligence, in order to provide inputs to the "Track & Manage Resource Trouble" process.</p>
<p>Extended Description:</p> <p>This process is responsible for categorizing the resource trouble according to the type of the trouble, impact, and standardized criteria at RM&O level. Moreover, this activity will be carried out with appropriate diligence, in order to provide inputs to the "Track & Manage Resource Trouble" process. <A></p>
<p>CENX Compliance</p> <p>Upon receiving a resource trouble notification through an alarm or an alert, CENX’s Real-time Troubleshooting module will qualify and classify the trouble as described in The Product Description Section 2.5.1. A message is then provided to external applications such as the Track&Manage Resource Trouble processes through the Northbound Interface as described in Product Description Section 2.5.8. <A></p>

4.3.3 Level 3: 1.5.8.6 - Close Resource Trouble Report

LEVEL 3 PROCESS MAPPING DETAILS 1.5.8.6 – Close Resource Trouble Report
Brief Description: Close a resource trouble report when the resource problem has been resolved.
Extended Description: The objective of the Close Service Trouble Report processes is to close a service trouble report when the service problem has been resolved. <A1> These processes monitor the status of all open service trouble reports, and recognize that a service trouble report is ready to be closed when the status is changed to cleared. <A2>
CENX Compliance As described in the response for 1.5.8.7.1, CENX will create a new resource trouble report as a result of resource alarm event notification analysis, and subsequent creation of new resource alarm event records, undertaken by the Survey & Analyze Resource Trouble processes. The state of that alarm and subsequent resource trouble report are tracked in CENX and updates to the state of that alarm and subsequent Resource Trouble Report are reported through the Northbound API (Product Description Section 2.5.8) and presented to users of the CENX Visualization portal as shown in supporting screenshot 5.8.1-3. When the alarm is abated, state of the resource is returned to healthy (assuming no other alarms exist) and a notification is generated on the Northbound API. <A1/A2> Analytic processes can be configured on the status of all alarms and resource troubles within the CENX Topology

4.3.4 Level 3: 1.5.8.7 - Create Resource Trouble Report

LEVEL 3 PROCESS MAPPING DETAILS 1.5.8.7 – Create Resource Trouble Report
Brief Description: Create a new resource trouble report.
Extended Description: The objective of the Create Resource Trouble Report process is to create a new resource trouble report. A new resource trouble report may be created as a result of resource alarm event notification analysis, and subsequent creation of new resource alarm event records, undertaken by the Survey & Analyze Resource Trouble processes, or at the request of analysis undertaken by other processes in the RM&O, SM&O (in particular a Service Trouble Report can generate one or more Resource Trouble Reports) or S/PRM layers which detect that some form of failure has occurred for which resource restoration activity is required to restore normal operation. If the resource trouble report is created as a result of a notification or request from processes other than the Survey & Analyze Resource Trouble processes, the Create Resource Trouble Report processes are responsible for converting the received information into a form suitable for the Resource Trouble Management processes, and for requesting additional information if required. These processes will make estimates of the time to restore resource which will be included in the new resource trouble report so that other processes can gain access to this information.
CENX Compliance (L3 process with L4 Definitions – see L4 Responses)

4.3.4.1 *Level 4: 1.5.8.7.1 - Generate Resource Trouble*

LEVEL 4 PROCESS MAPPING DETAILS 1.5.8.7.1 – Generate Resource Trouble
Brief Description: This process creates a new resource trouble report.<A>
Extended Description: Not used for this process element
CENX Compliance A new resource trouble report may be created as a result of resource alarm event notification analysis, and subsequent creation of new resource alarm event records, undertaken by the Survey & Analyze Resource Trouble processes. With each trouble – the report defines the set of all customer services impacted by the given trouble. The supporting screenshot from 5.8.1-3 shows a resource trouble report including all alerts on the impacted resource elements. The list may be filtered by region or specific resource element.

4.3.4.2 *Level 4: 5.8.7.2 - Convert Report To Resource Trouble Format*

LEVEL 4 PROCESS MAPPING DETAILS	
1.5.8.7.2 – Convert Report to Resource Trouble Format	
Brief Description:	If the resource trouble report is created as a result of a notification or request from processes other than the Survey & Analyze Resource Trouble processes, this process is responsible for converting the received information into a form suitable for the Resource Trouble Management processes, and for requesting additional information if required. <A>
Extended Description:	Not used for this process element
CENX Compliance	CENX generates and provides a resource trouble report to external applications that may perform resource trouble management functions through the Northbound Interface as described in the Product Description 2.5.8.

4.3.4.3 *Level 4: 1.5.8.7.3 - Estimate Time for Restoring Resource*

LEVEL 4 PROCESS MAPPING DETAILS 1.5.8.7.3 – Estimate Time For Restoring Resource	
Brief Description:	This process estimates the time to restore service which is included in the new Service Trouble report so that other processes can gain access to this information. <M>
Extended Description:	Not used for this process element
CENX Compliance	CENX does not provide out of the box capability for determining the time to restore the service. However, through configuration and customization, the resource problem could be readily extended using data from the CENX data store to determine average resolution time for similar issues and provide estimated resolution duration. <M>

4.3.5 Supporting Evidence References

- Exanova_6.1_Service Intelligence Product Description.pdf
- cenx_exanova_6.1_core_users_guide.pdf
- eTOM 5-8 Resource Trouble Management - CENX Conformance - supporting Screen Shots v0-1.pdf

4.3.6 Level 4/Level 3 Detailed Scores

Table 4-3 1.5.8 Resource Trouble Management– Level 4 & Level 3 Scores

CENX V6.1 Framework 16.0 Business Process Framework Conformance Scores	
1.5 - Resource Domain	
Level 2: 1.5.8 - Resource Trouble Management	Conformance
1.5.8.1 - Survey & Analyze Resource Trouble	5
1.5.8.1.1 – Manage Resource Alarm Event Notifications	100%
1.5.8.1.2 – Filter Resource Alarm Event Notifications	100%
1.5.8.1.3 – Correlate Resource Alarm Event Notifications	100%
1.5.8.1.4 – Abate Alarm Event Records	100%
1.5.8.1.5 – Trigger Defined Action	100%
1.5.8.1.6 – Monitor Resource Alarms Events	100%
1.5.8.1.7 – Categorize Resource Alarm Event	100%
1.5.8.2 - Localize Resource Trouble	5
1.5.8.2.1 – Verify Resource Configuration	100%
1.5.8.2.2 – Perform Specific Resource Trouble Diagnostics	100%
1.5.8.2.3 – Perform Specific Resource Trouble Tests	100%
1.5.8.2.4 – Stop And Start Audit On Resources	100%
1.5.8.2.5 – Schedule Routine Resource Trouble Tests	100%
1.5.8.2.6 – Notify T&M Root Cause Resource Trouble	100%
1.5.8.2.7 – Categorize Resource Trouble	100%
<i>1.5.8.3 - Correct & Resolve Resource Trouble</i>	<i>Not in Scope</i>
<i>1.5.8.4 - Track & Manage Resource Trouble</i>	<i>Not in Scope</i>
<i>1.5.8.5 - Report Resource Trouble</i>	<i>Not in Scope</i>
1.5.8.6 - Close Resource Trouble Report	5
1.5.8.7 - Create Resource Trouble Report	5
1.5.8.7.1 – Generate Resource Trouble	100%
1.5.8.7.2 – Convert Report To Resource Trouble Format	100%
1.5.8.7.3 – Estimate Time For Restoring Resource	25%

4.4 Level 2: 1.5.9 – Resource Performance Management

4.4.1 Level 3: 1.5.9.1 - Monitor Resource Performance

LEVEL 3 PROCESS MAPPING DETAILS 1.5.9.1 - Monitor Resource Performance	
Brief Description:	Monitor received resource performance information and undertake first-in detection.
Extended Description:	<p>The objective of the Monitor Resource Performance processes is to monitor received resource performance information and undertake first-in detection.</p> <p>The responsibilities of the processes include, but are not limited to:</p> <ul style="list-style-type: none">•Undertaking the role of first in detection by monitoring the received specific resource performance data;•Comparing the received specific resource performance data to performance standards set for each specific resource (available from the Resource Inventory);•Assessing and recording received specific resource performance data which is within tolerance limits for performance standards, and for which continuous monitoring and measuring of specific resource performance is required;•Recording the results of the continuous monitoring for reporting through the Report Resource Performance processes;•Detecting performance threshold violations which represent specific resource failures due to abnormal performance;•Passing information about resource failures due to performance threshold violations to Resource Trouble Management to manage any necessary restoration activity as determined by that process;•Passing information about potential specific service performance degradations arising from specific resource degradations to Service Quality Management to manage any necessary restoration activity as determined by that process;•Detecting performance degradation for specific resources which provide early warning of potential issues;•Forwarding resource performance degradation notifications to other Resource Performance Management processes, which manage activities to restore normal specific resource performance•Logging specific resource performance degradation and violation details within the repository in the Manage Resource Inventory processes to ensure historical records are available to support

the needs of other processes.

CENX Compliance

This is a Level 3 process – please see details in Level 4 processes.

4.4.1.1 *Level 4: 1.5.9.1.1 - Manage Resource Performance Data*

LEVEL 4 PROCESS MAPPING DETAILS 1.5.9.1.1 - Manage Resource Performance Data
<p>Brief Description:</p> <p>This process monitors and logs the received specific resource performance quality data <A1>, compares the received specific resource performance data to performance standards set for each specific resource (available from the Resource Inventory), detects performance threshold violations which represent specific resource failures due to abnormal performance, and detects performance degradation for specific resources which provide early warning of potential issues. <A2> This process undertakes the role of first in detection by monitoring the received specific resource performance data; <A3></p>
<p>Extended Description:</p> <p>Not used for this process element.</p>
<p>CENX Compliance</p> <p>CENX is responsible for the management, persistence and analytics of Resource Performance data. CENX has been used for a wide array of performance data as described in the Product Description, Section 2.6.</p> <p style="padding-left: 40px;">The CENX Network Analytics Module is an advanced tool for managing and optimizing network designs leveraging comprehensive utilization and performance data from the network across multiple data sources.</p> <p>Examples of this data are described in the product document for L2/L3 Switches, Mobile Backhaul, Radio Access Networks, Microwave Transmission and optical networks (Section 2.6.1.1-2.6.1.4).</p> <p>The supporting screenshots (Section 5.9.1 – screenshot 1 and 2) show representation of the various performance data from the resources delivering a service. Screenshot 1 shows resource performance for a Radio access network and Screenshot 2 shows the data for Ethernet backhaul network. <A1></p> <p>Using Threshold Crossing alerts, CENX will analyze the resource performance data and generate alarms or alerts based on the configured thresholds for the resource or related services. Threshold crossing alert capabilities is described in the Product Description Section 2.6.1 <A2></p> <ul style="list-style-type: none">• Analysis of performance and utilization data showing trends and triggering events including generation of alarms based on rule violations such as<ul style="list-style-type: none">○ Threshold crossing events – where measurements over a threshold trigger the creation of an alarm○ Hold On/Hold Off rules – where several samples above or below a threshold will trigger the creation or release of an alarm.

- Considerations for Planning Maintenance Activities

The alarms generated through the performance data analytics will generate an alarm and escalate that alarm to the appropriate resource trouble or service problem management systems through the CENX Northbound Interface as described in the Product Description Section 2.5.8. <A3>

4.4.1.2 *Level 4: 1.5.9.1.2 - Record Resource Performance Data*

LEVEL 4 PROCESS MAPPING DETAILS 1.5.9.1.2 - Record Resource Performance Data
<p>Brief Description:</p> <p>This process assesses and records received specific resource performance data which is within tolerance limits for performance standards, and for which continuous monitoring and measuring of specific resource performance is required. <A1> It records the results of the continuous monitoring for reporting through the Report Resource Performance processes, and logs specific resource performance degradation and violation details within the repository in the Manage Resource Inventory processes to ensure historical records are available to support the needs of other processes. <A2></p>
<p>Extended Description:</p> <p>Not used for this process element.</p>
<p>CENX Compliance</p> <p>CENX Suite assesses and records specific resource performance data and analyses the data to ensure it is within tolerance levels defined at the resource or related service metrics. The capability in support of this process is by the CENX Network Analytics module as described in Section 2.6 of the Product Description. Data is gathered and analyzed (or assessed) to ensure tolerance through the Threshold Crossing Alerts configuration rules (Section 2.6.1). <A1></p> <p>The data is logged and made available for reporting and presentation as shown in the reference screenshots – Section 5.9.1 – screenshot 1 and 2. Violation of Service Level Agreements, Resource thresholds, or other alerts are configured and posted to other interested processes through the CENX Northbound Interface – as describe3d in the Product Description Section 2.5.8. <A2></p>

4.4.1.3 *Level 4: 1.5.9.1.3 - Correlate Resource Performance Event Notifications*

LEVEL 4 PROCESS MAPPING DETAILS 1.5.9.1.3 - Correlate Resource Performance Event Notifications
<p>Brief Description:</p> <p>This process passes information about potential specific service performance degradations arising from specific resource degradations to Service Quality Management to manage any necessary restoration activity as determined by that process. <A1> It passes information about resource failures due to performance threshold violations to Resource Trouble Management to manage any necessary restoration activity as determined by that process. <A2> It forwards resource performance degradation notifications to other Resource Performance Management processes, which manage activities to restore normal specific resource performance. <A3></p>
<p>Extended Description:</p> <p>Not used for this process element.</p>
<p>CENX Compliance</p> <p>The CENX Suite identifies and generates resource performance event notifications and correlates them with other events with coordination to CENX's own Resource Trouble Management application or to external process through the Northbound Interface.</p> <p>Once a resource performance degradation event has been detected through CENX Threshold Crossing Alert capability of the Network Analytics module (Product Description 2.6.1) the event is decorated with information sourced in the CENX Service Information model (Product Description 2.2) and published through the northbound interface (Product Description 2.5.8) for processing by external Service Quality Management applications. Either CENX's Resource Trouble Management, CENX's Service Quality Management or an external application will receive this event and manage it for initiating and tracking restoration activities. <A1/A2/A3></p>

4.4.2 Level 3: 1.5.9.5 – Create Resource Performance Degradation Report

LEVEL 3 PROCESS MAPPING DETAILS 1.5.9.5 - Create Resource Performance Degradation Report
Brief Description: Create a new resource performance degradation report
Extended Description: <p>The objective of the Create Resource Performance Degradation Report process is to create a new resource performance degradation report, modify existing resource performance degradation reports, and request cancellation of existing resource performance degradation reports.</p> <p>A new resource performance degradation report may be created as a result of specific resource performance notifications undertaken by the Monitor Resource Performance processes, or at the request of analysis undertaken by other RM&O, SM&O or party management processes which detect that some form of deterioration or failure has occurred requires an assessment of the specific resource performance.</p> <p>If the resource performance degradation report is created as a result of a notification or request from processes other than Monitor Resource Performance processes, the Create Resource Performance Degradation Report processes are responsible for converting the received information into a form suitable for the Resource Performance Management processes, and for requesting additional information if required.</p>
CENX Compliance This is a Level 3 process – please see details in Level 4 processes.

4.4.2.1 *Level 4: 1.5.9.5.1 - Generate Resource Performance Degradation Problem*

LEVEL 4 PROCESS MAPPING DETAILS 1.5.9.5.1 - Generate Resource Performance Degradation Problem
Brief Description: This process creates a new Resource Performance Degradation Report as a result of specific resource performance notifications undertaken by the Monitor Resource Performance processes, <A1> or at the request of analysis undertaken by other RM&O, SM&O or RM&O processes which detect that some form of deterioration or failure has occurred requires an assessment of the specific resource performance. <A2>
Extended Description: Not used for this process element.
CENX Compliance CENX suite provides a comprehensive set of capabilities for generating reports and dashboards on resource performance data and resource performance violations. Attached screenshot 5.9.5 screenshot-1 shows a report based on Frame loss performance data analysis. CENX identified numerous resource performance violations and made each one available for analysis and review in this report. Users may see details of the individual resource performance degradation reports, or a macro view across regions, providers, sites etc. <A1> CENX makes the performance data available for users to explore, analyze, and assess resource data. At the request of other processes, users may utilize the CENX dashboards and reports to examine the performance data in unique ways to qualify or quantify a perceived issue or to investigate network anomalies. An example of this is shown in the screenshots Section 5.9.5 – screenshot 2 where users can interrogate L2 network performance data to investigate various resource performance. <A2>

4.4.2.2 *Level 4: 1.5.9.5.2 - Convert Report to Resource Performance Degradation Report Format*

LEVEL 4 PROCESS MAPPING DETAILS	
1.5.9.5.2 - Convert Report to Resource Performance Degradation Report Format	
Brief Description:	If the resource performance degradation report is created as a result of a notification or request from processes other than Monitor Resource Performance processes, this process responsible for converting the received information into a form suitable for the Resource Performance Management processes, and for requesting additional information if required. <A>
Extended Description:	Not used for this process element.
CENX Compliance	As described in Generate Resource Performance Degradation Report (5.9.5.1), part A2, CENX makes the resource performance data available for analysis through a comprehensive set of dashboards and reports. The data analyzed through these reports can be extracted or exported into a variety of external formats including Excel/CSV, PDF for image as described in the Product Description Section 2.7.1.

4.4.3 Level 3: 1.5.9.7- Close Resource Performance Degradation Report

LEVEL 3 PROCESS MAPPING DETAILS 5.9.7 – Close Resource Performance Degradation Report
Brief Description: Close a resource performance degradation report when the resource performance has been resolved.<A>
Extended Description: The objective of the Close Resource Performance Degradation Report processes is to close a resource performance degradation report when the resource performance has been resolved. These processes monitor the status of all open resource performance degradation reports, and recognize that a resource performance degradation report is ready to be closed when the status is changed to cleared.
CENX Compliance CENX will close a resource performance degradation report when the resource returns to normal levels. This is performed through the Threshold Crossing Alerts (TCAs) and hold-on/hold-off rules as defined in the Product Description Section 2.6.1. When a resource performance metric has crossed a threshold, more than the number of 'hold-off' times an alert is generated and decorated into a degradation report as described in 5.9.5. When the performance falls below the threshold, up to the number of hold-on times then the alarm is released and the corresponding Degradation report is removed. The occurrence of the degradation alarm is available for analysis but it is now in a resolved status.

4.4.4 Supporting Evidence References

- CENX_6-1 Service Intelligence Product Description.pdf
- eTOM 5-9 Resource Performance Management - CENX Conformance - supporting Screen Shots v0-1.pdf

4.4.5 Level 4/Level 3 Detailed Scores

Table 4-4 1.5.9 Resource Performance Management– Level 4 & Level 3 Scores

CENX V6.1 Framework 16.0 Business Process Framework Conformance Scores		
1.5 - Resource Domain		
Level 2: 1.5.9 - Resource Performance Management		Conformance
1.5.9.1 - Monitor Resource Performance		5
	1.5.9.1.1 - Manage Resource Performance Data	100%
	1.5.9.1.2 - Record Resource Performance Data	100%
	1.5.9.1.3 - Correlate Resource Performance Event Notifications	100%
<i>1.5.9.2 - Analyze Resource Performance</i>		<i>Not in Scope</i>
<i>1.5.9.3 - Control Resource Performance</i>		<i>Not in Scope</i>
<i>1.5.9.4 - Report Resource Performance</i>		<i>Not in Scope</i>
1.5.9.5 - Create Resource Performance Degradation Report		5
	1.5.9.5.1 - Generate Resource Performance Degradation Problem	100%
	1.5.9.5.2 - Convert Report To Resource Performance Degradation Report Format	100%
<i>1.5.9.6 - Track & Manage Resource Performance Resolution</i>		<i>Not in Scope</i>
1.5.9.7 - Close Resource Performance Degradation Report		5

5 Information Framework Assessment Overview

5.1 Mapping Technique Employed

Not applicable for this assessment.

5.2 Information Framework Assessment - ABE Scope

Not applicable for this assessment.

5.3 Product Scope

Not applicable for this assessment.

6 Framework Conformance Result

This Section details the Scores awarded to reflect Conformance of the CENX product to the Business Process Framework & Information Framework components of Framework 16.0.

6.1 Business Process Framework – Scoring Rules

The conformance scores granted were based on the following TM Forum scoring rules:

Framework Conformance Scoring Guidelines Business Process Framework (eTOM): Conformance Scoring Guidelines		
Process Level	Conformance Score	Qualifier
Level 1 Process	Not applicable	<i>Conformance Assessment shall not be carried out at this process level.</i>
Level 2 Process	Not applicable	<i>A conformance level is not awarded to Level 2 processes in Framework Certification. The Certification Report shall highlight the coverage within a Level 2 process submitted in scope for an Assessment, in terms of number of Level 3 processes submitted for assessment out of the total number defined in the Business Process Framework for the Level 2 process.</i>
Level 3 Process	Conformance Score is awarded between 3.1 & 5.0	The Conformance Score is awarded for each Level 3 process submitted in scope for the Assessment. The Conformance Score awarded can be a value between 3.1* & 5 depending on the level of coverage & conformance to the Level 3 process based on the alignment to the level 3 Implied Tasks as decomposed in the Level 4 process definitions. If a Level 3 process has not been decomposed to Level 4 processes, the Level score is awarded according to alignment to the Level 3 defined Implied Tasks.
Level 4 Process	Level of conformance is calculated as input to parent Level 3 Process Score	<i>Levels of conformance are calculated for Level 4 processes according to alignment to the individual implied tasks. Level 4 scores are summed and averaged to given an overall score for the parent Level 3 process.</i>
* In earlier Conformance Assessments, scores were awarded to Level 1 & Level 2 processes using values 1 through to 3. For this reason, the Level 3 scores start from > 3.		

Figure 6-1 TM Forum Business Process Framework: Conformance Scoring Rules

Additional Notes on Business Process Framework Conformance Scoring

1. Level 1 processes shall be presented to define the assessment scope only. i.e. they shall not be assessed as self-contained processes since the level of detail is not considered sufficient.

A conformance level shall not be awarded for Level 1 processes.

2. Level 2 processes shall be presented to define the assessment scope only. i.e. they shall not be assessed as self-contained processes since the level of detail is not considered sufficient.

A conformance level shall not be awarded for Level 2 processes. However, the Certification Report shall provide good indication of the coverage of the Level 2 process in terms of number of contained Level 3 processes submitted in scope for the Assessment.

3. The Conformance Assessment shall be carried out at process level 3. For each Level 3 process, conformance shall be deduced according to the support for the process implied tasks, as decomposed and described in the underlying Level 4 process descriptions. The score awarded for a Level 3 process, is deduced according to the support mapped to the Level 4 processes/Implied Tasks. This provides finer granularity of scoring than in Assessment prior to Framework 12.0 based Assessments.

4. In evaluating conformance to the standards, manual intervention shall not impact the conformance score granted. However, any level of manual support shall be noted in the Conformance Report and Detailed Results Report. This note specifically applies to Product & Solution Assessments.

5. Processes that are supported via manual implementation only, are not considered in scope for the Assessment. This note specifically applies to Product & Solution Assessments.

6.2 Business Process Framework – Conformance Result Summary

The graph in this Section provides an overview of the conformance levels granted to the Level 3 Processes presented in scope for the CENX Assessment. Each Level 3 process was measured using a Business Process Framework (eTOM) conformance score according to level of Conformance – Full Conformance or Partial Conformance as described in Section 6.1 Business Process Framework – Scoring Rules.

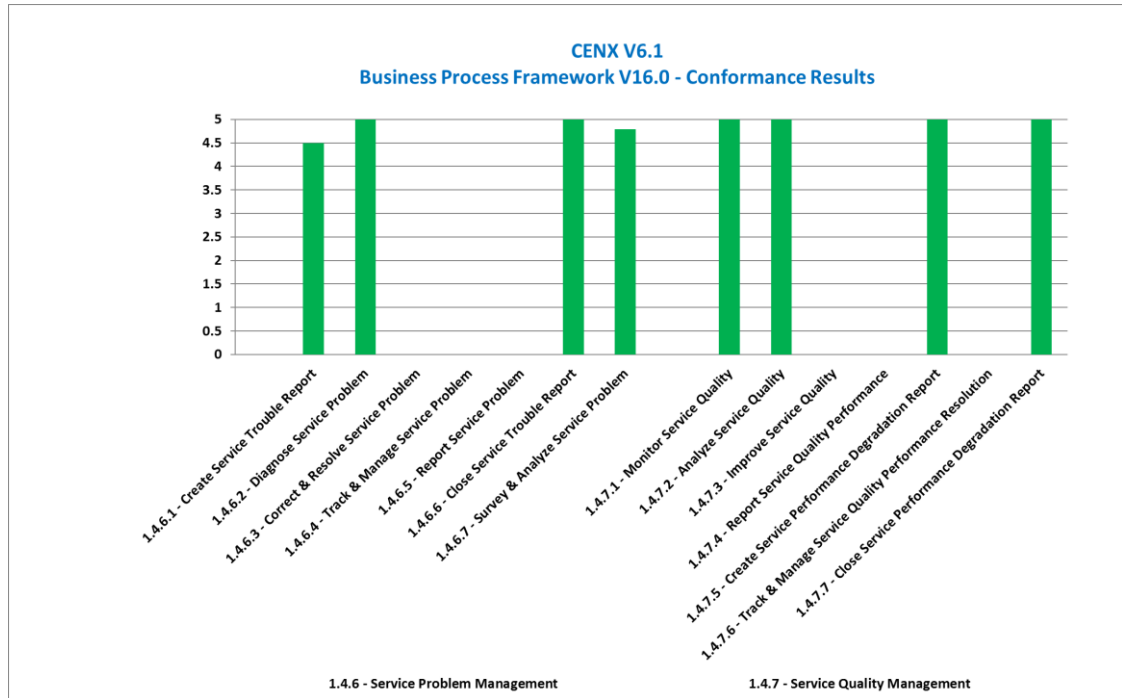


Figure 6-2 Business Process Framework: Conformance Results Service Domain

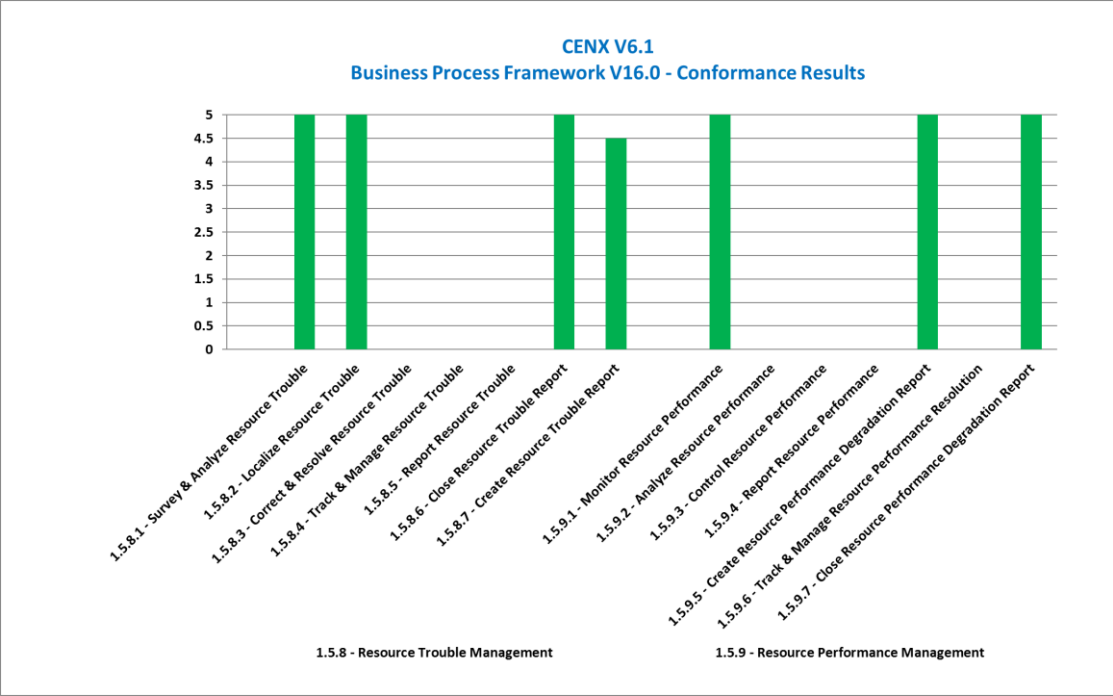


Figure 6-3 Business Process Framework: Conformance Result Resource Domain

6.3 Business Process Framework – Detailed Conformance Results

The following table provides a more detailed breakdown of the scores awarded with some additional commentary

Table 6-1 Business Process Framework: Detailed Conformance Results

CENX V6.1 Business Process Framework (eTOM) Release 16.0 Conformance		
L1 / L2 / L3 Process	L3 Process Score [L2 Coverage]	Comments
Service Domain		
Level 2: 1.4.6 - Service Problem Management	[4/7]	
1.4.6.1 - Create Service Trouble Report	4.5	Partially Conformant Supporting evidence and documentation submitted for the assessment of this level 3 process fulfilled alignment criteria with the standard Business Process Framework (eTOM) but with some deviations. See Level 3/Level 4 results Section in Chapter 4.
1.4.6.2 - Diagnose Service Problem	5.0	Fully Conformant Supporting evidence and documentation submitted for the assessment of this level 3 process fulfilled alignment criteria with the standard Business Process Framework (eTOM).
<i>1.4.6.3 - Correct & Resolve Service Problem</i>	<i>Not in Scope</i>	<i>This process was not submitted for assessment.</i>
<i>1.4.6.4 - Track & Manage Service Problem</i>	<i>Not in Scope</i>	<i>This process was not submitted for assessment.</i>
<i>1.4.6.5 - Report Service Problem</i>	<i>Not in Scope</i>	<i>This process was not submitted for assessment.</i>
1.4.6.6 - Close Service Trouble Report	5	Fully Conformant Supporting evidence and documentation submitted for the assessment of this level 3 process fulfilled alignment criteria with the

		standard Business Process Framework (eTOM).
1.4.6.7 - Survey & Analyze Service Problem	4.8	Partially Conformant Supporting evidence and documentation submitted for the assessment of this level 3 process fulfilled alignment criteria with the standard Business Process Framework (eTOM) but with some deviations. See Level 3/Level 4 results Section in Chapter 4.
Level 2: 1.4.7 - Service Quality Management	[4/7]	
1.4.7.1 - Monitor Service Quality	5.0	Fully Conformant Supporting evidence and documentation submitted for the assessment of this level 3 process fulfilled alignment criteria with the standard Business Process Framework (eTOM).
1.4.7.2 - Analyze Service Quality	5.0	Fully Conformant Supporting evidence and documentation submitted for the assessment of this level 3 process fulfilled alignment criteria with the standard Business Process Framework (eTOM).
<i>1.4.7.3 - Improve Service Quality</i>	<i>Not in Scope</i>	<i>This process was not submitted for assessment.</i>
<i>1.4.7.4 - Report Service Quality Performance</i>	<i>Not in Scope</i>	<i>This process was not submitted for assessment.</i>
1.4.7.5 - Create Service Performance Degradation Report	5.0	Fully Conformant Supporting evidence and documentation submitted for the assessment of this level 3 process fulfilled alignment criteria with the standard Business Process Framework (eTOM).
<i>1.4.7.6 - Track & Manage Service Quality Performance Resolution</i>	<i>Not in Scope</i>	<i>This process was not submitted for assessment.</i>

1.4.7.7 - Close Service Performance Degradation Report	5.0	Fully Conformant Supporting evidence and documentation submitted for the assessment of this level 3 process fulfilled alignment criteria with the standard Business Process Framework (eTOM).
Resource Domain		
Level 2: 1.5.8 - Resource Trouble Management	[4/7]	
1.5.8.1 - Survey & Analyze Resource Trouble	5.0	Fully Conformant Supporting evidence and documentation submitted for the assessment of this level 3 process fulfilled alignment criteria with the standard Business Process Framework (eTOM).
1.5.8.2 - Localize Resource Trouble	5.0	Fully Conformant Supporting evidence and documentation submitted for the assessment of this level 3 process fulfilled alignment criteria with the standard Business Process Framework (eTOM).
<i>1.5.8.3 - Correct & Resolve Resource Trouble</i>	<i>Not in Scope</i>	<i>This process was not submitted for assessment.</i>
<i>1.5.8.4 - Track & Manage Resource Trouble</i>	<i>Not in Scope</i>	<i>This process was not submitted for assessment.</i>
<i>1.5.8.5 - Report Resource Trouble</i>	<i>Not in Scope</i>	<i>This process was not submitted for assessment.</i>
1.5.8.6 - Close Resource Trouble Report	5.0	Fully Conformant Supporting evidence and documentation submitted for the assessment of this level 3 process fulfilled alignment criteria with the standard Business Process Framework (eTOM).
1.5.8.7 - Create Resource Trouble Report	4.5	Partially Conformant Supporting evidence and documentation submitted for the assessment of this level 3 process fulfilled alignment criteria with the standard Business Process Framework (eTOM) but with some deviations. See

		Level 3/Level 4 results Section in Chapter 4.
Level 2: 1.5.9 - Resource Performance Management	[3/7]	
1.5.9.1 - Monitor Resource Performance	5.0	Fully Conformant Supporting evidence and documentation submitted for the assessment of this level 3 process fulfilled alignment criteria with the standard Business Process Framework (eTOM).
<i>1.5.9.2 - Analyze Resource Performance</i>	<i>Not in Scope</i>	<i>This process was not submitted for assessment.</i>
<i>1.5.9.3 - Control Resource Performance</i>	<i>Not in Scope</i>	<i>This process was not submitted for assessment.</i>
<i>1.5.9.4 - Report Resource Performance</i>	<i>Not in Scope</i>	<i>This process was not submitted for assessment.</i>
1.5.9.5 - Create Resource Performance Degradation Report	5.0	Fully Conformant Supporting evidence and documentation submitted for the assessment of this level 3 process fulfilled alignment criteria with the standard Business Process Framework (eTOM).
<i>1.5.9.6 - Track & Manage Resource Performance Resolution</i>	<i>Not in Scope</i>	<i>This process was not submitted for assessment.</i>
1.5.9.7 - Close Resource Performance Degradation Report	5.0	Fully Conformant Supporting evidence and documentation submitted for the assessment of this level 3 process fulfilled alignment criteria with the standard Business Process Framework (eTOM).

6.4 Information Framework – Scoring Rules

Not applicable for this assessment.

6.4.1 Information Framework Maturity Conformance Scoring Methodology

Not applicable for this assessment.

6.4.2 Information Framework Adoption Conformance Scoring Methodology

Not applicable for this assessment.

6.5 Information Framework – Conformance Result Summary

Not applicable for this assessment.

6.5.1 Information Framework - Maturity Conformance Result Summary

Not applicable for this assessment.

6.5.2 Information Framework - Adoption Conformance Result Summary

Not applicable for this assessment.

6.6 Information Framework – Detailed Conformance Result

Not applicable for this assessment.