CSP CIOs Address 3 Key Challenges to Modernize Service and Network Assurance

Published 12 December 2023 - ID G00800625 - 9 min read

By Analyst(s): Susan Welsh de Grimaldo

Initiatives: CSP Digital Transformation and Innovation

Driving strategic business outcomes — revenue growth, cost savings, improved CX — demands new capabilities and architectures for service and network assurance. CSP CIOs need to address key challenges to guide assurance transformation decisions, including vendor and solution evaluation and selection.

Overview

Key Findings

- Chief technology and information officers are challenged to determine the best approach to improve service and network assurance capabilities while optimizing total cost of ownership, particularly if they are aiming for consolidation of multiple legacy assurance solutions.

- Assurance decisions are also critical to enable new and enhanced services for revenue growth, such as in efforts to drive 5G monetization with network slicing and the introduction of new secure access service edge (SASE) offers.

- Assurance solutions currently in use at many communications service providers (CSPs) lack the capabilities and scale needed to support new operating models and roadmaps. The solutions are also unable to support network and service complexity and a push to increase automation and intelligence in service and network operations.

Recommendations

- Clarify your target goals, the current state of assurance, and your investment (and risk) levels and timing to determine the best approach to transform assurance capabilities.
- Enable priority business outcomes with service and network assurance transformation by working with key stakeholders from multiple teams, including lines of business. Include relevant KPIs to measure the effect on targeted business outcomes.
- Plan service and network assurance (S&NA roadmap) and architecture to support evolving networks, services and operating model change. Evaluate and partner with vendors to support your roadmap.

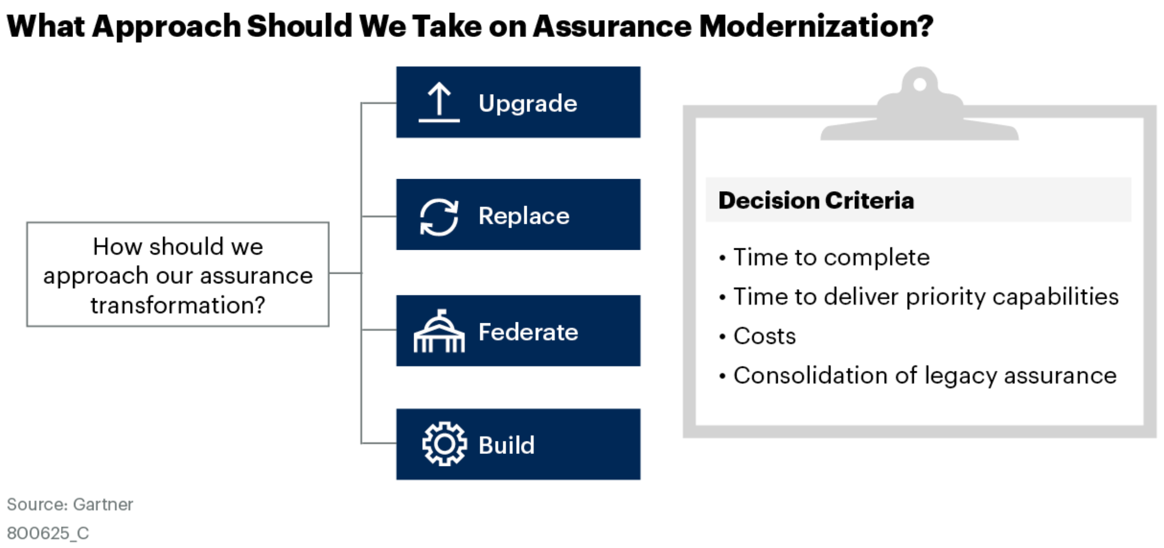
Introduction

As communications service provider (CSP) chief information officers (CIOs) and other tech leaders plan for evolving S&NA capabilities to address business priorities and growing network complexities, they face three key challenges, addressed by these questions:

- What is the best approach to S&NA modernization?
- How do we enable key business outcomes with S&NA?
- What is needed in our S&NA roadmap and architecture to enable new operating models?

These three questions are intertwined and should be considered in conjunction with one another to guide assurance transformation decisions, including vendor and solution evaluation and selection.

Figure 1: What Approach Should We Take on Assurance Modernization?


What Approach Should We Take on Assurance Modernization?
How should we approach our assurance transformation?
Upgrade
Replace
Federate
Build
Decision Criteria
• Time to complete
• Time to deliver priority capabilities
• Costs
• Consolidation of legacy assurance
Source: Gartner
800625_C
Gartner

Analysis

Challenge No. 1: Determine the Best Approach to Transform Assurance Capabilities

A key challenge CSP chief technology information officers (CTIOs) face as they plan to transform assurance capabilities to meet new requirements is determining how to acquire the new capabilities and whether to do so all at once or incrementally. The optimal approach will depend on a number of factors and will not be the same for all CSPs. Decisions need to take into account investment levels and timing, ways to optimize total cost of ownership (TCO) and manage risks, and how to deliver growth and network and service improvements that drive better customer experience (CX). Additional factors must also be considered, such as which solutions are currently deployed and how the solution providers are addressing potential upgrades (such as are the solutions end-of-life, legacy products or newer products with R&D investment supporting new releases).

CTIOs must decide — based on the current state of their assurance, target goals and investment (and risk) levels and timing — whether it is best to:

- **Upgrade** their existing legacy solutions (which may be self-developed or procured solutions, or a combination). This approach can aim to add incremental improvements, but could be costly and inefficient; the process could include some consolidation of current assurance solutions. Taking an upgrade approach may be a good option if there is a clear roadmap and ongoing development of existing solutions.

- **Fully replace** current systems, in a large full transformation project; the new solutions could be delivered in a SaaS model as one option. For CSPs with the budget and appetite, and the need to fully revamp capabilities, this can be an option to consider. Successful delivery will require close collaboration with solutions providers to ensure existing services are not negatively affected, that transition precursors are adequately addressed (such as data management and feeds) and that project milestones are met in a timely fashion.

- **Federate** existing capabilities while adding incremental new functionalities and gradually replacing and consolidating older elements; this could potentially use a SaaS model. This approach can be useful if a CSP has a range of assurance solutions (such as multiple solutions acquired through mergers and acquisitions with other CSPs) that are functioning but lack specific capabilities needed for new services.

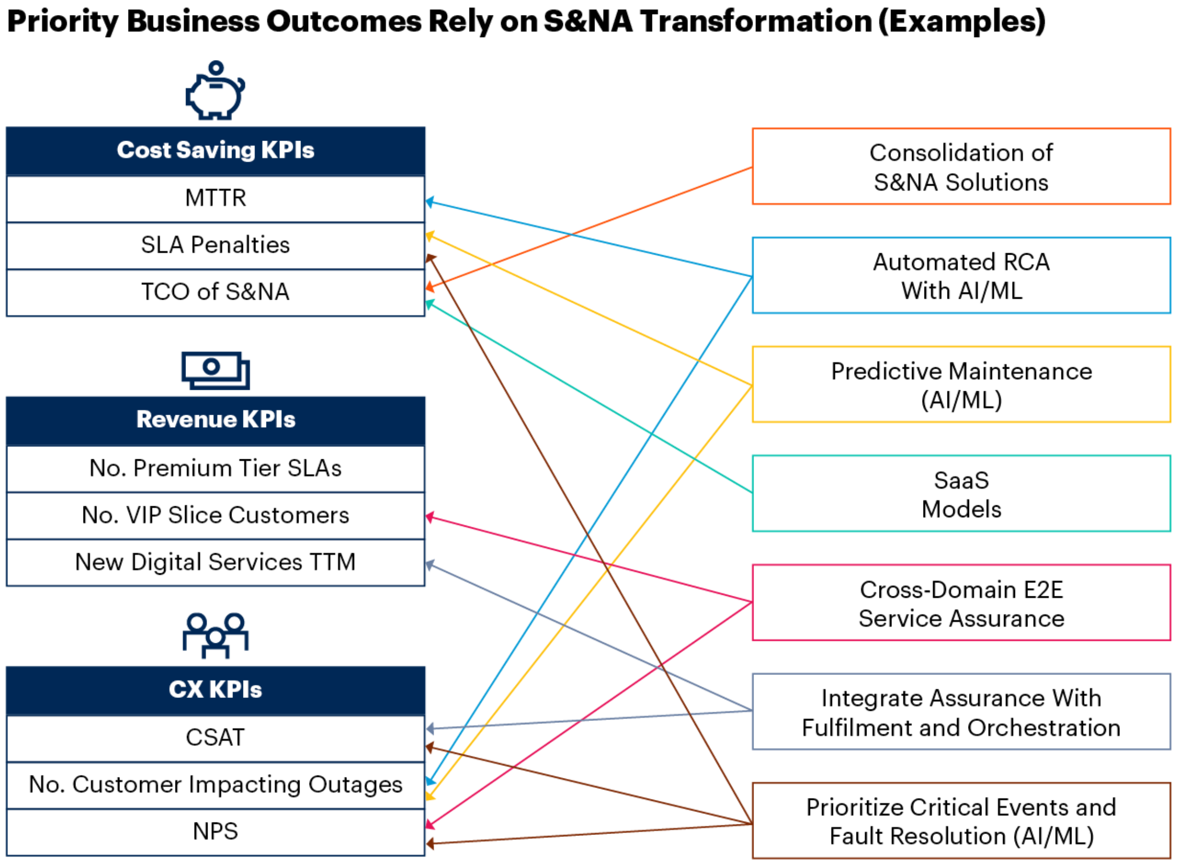
- **Build** new capabilities in-house to supplement or replace existing assurance solutions. CSPs with strong in-house development capabilities could consider this route, or build some capabilities while acquiring others from solutions partners.

Determining the best approach should also take into consideration the requirements that are identified as the next two challenges are addressed.

Challenge No. 2: Enable Priority Business Outcomes With Service and Network Assurance Transformation

With networks and services increasing in complexity as they evolve, it is essential to implement newer capabilities and architectures in S&NA to enable strategic business needs beyond keeping networks and services running. CTIOs must identify which business outcomes need to be enabled through assurance modernization, and how progress toward delivering on the outcomes will be measured. Figure 2 portrays a sample range of strategic business outcomes — cost savings, revenue generation and improved CX — and related key performance indicators (KPIs) and S&NA transformation project capabilities that support them.

Figure 2: Priority Business Outcomes Rely on S&NA Transformation (Examples)


Priority Business Outcomes Rely on S&NA Transformation (Examples)
Cost Saving KPIs
MTTR
SLA Penalties
TCO of S&NA
Revenue KPIs
No. Premium Tier SLAs
No. VIP Slice Customers
New Digital Services TTM
CX KPIs
CSAT
No. Customer Impacting Outages
NPS
Consolidation of S&NA Solutions
Automated RCA With AI/ML
Predictive Maintenance (AI/ML)
SaaS Models
Cross-Domain E2E Service Assurance
Integrate Assurance With Fulfilment and Orchestration
Prioritize Critical Events and Fault Resolution (AI/ML)

Source: Gartner
764503_C

CTIOs should identify the prioritization for S&NA capabilities modernization based on interactions with key stakeholders to ensure new capabilities will deliver on the KPIs and outcomes that lines of business and other stakeholders want to improve. CTIOs should incorporate processes to measure and communicate the impact of S&NA capabilities on these prioritized business goals.

Challenge No. 3: Plan S&NA Roadmap and Architecture to Support Evolving Networks, Services and Operating Model Change

CSP CTIOs need to build a detailed roadmap for S&NA modernization, collaborating with solution vendors, to address required capabilities, in-house skills development and process changes. Through this, CTIOs can deliver on evolving business needs and enable desired business outcomes. As part of the planning, incorporate steps to increase automation and intelligence, and a target architecture for integration with enhanced inventory, orchestration and service design for end-to-end (E2E) service life cycle management (LCM) and new operating models. Ensure that capabilities support progression from reactive issue resolution to proactive and predictive management of both networks and services (including SLAs) across network domains and layers. Explore further guidance from Gartner on operations support system (OSS) and assurance architecture evolution in Objectives and Principles for Assurance Architecture Evolution in CSPs and Objectives and Principles for OSS Architecture Evolution in CSPs.

Evaluating and Partnering With Vendors to Support Your Roadmap

In selecting and partnering with solution vendors, evaluate how well their current and evolving assurance architecture, capabilities and best practices align with your requirements and goals. S&NA solution vendors are increasingly:

- **Focusing on data inputs and management**: Successful assurance transformation relies on real-time access to a wide range of data on service and network performance:
  - Incorporating both centralized elements and capabilities on the edge to minimize cost and timeliness of data transport, processing and storage in the cloud.
  - Integration with continuous active testing for proactive management of service-level agreements triggering assurance actions.
  - Capability to ingest data from distributed and E2E topology and additional sources.

- **Converging OSS with network and moving to cloud:**
  - Preparing for new radio access network (RAN) architectures, such as vRAN and Open RAN (with the near-real-time radio intelligent controller [RIC] providing some assurance-related functions in the O-RAN ALLIANCE architecture).
  - Prioritizing S&NA areas closer to service and customer experience in a gradual move to the cloud (such as management of SLAs).
  - Converging management (orchestration and assurance) for physical and virtual network resources, as networks incorporate telco cloud.
- **Increasing full visibility and improved observability:**
  - Supporting multilayer, multidomain hybrid environments, with visibility into the infrastructure layer up to the service and applications layer in cloud-based networks.
  - Supporting netco and servco since network operations centers (NOCs) and service operations centers (SOCs) are separate but need 360-degree assurance for E2E correlation across network and service performance and customer experience.
  - Using digital twin models of the network to support predictive actions and simulate situations in the network to anticipate issues (such as likely data traffic impact of a new promotion).
  - Using open APIs to support modular, composable open architecture with visibility across multivendor networks and capabilities to extend observability from internal teams to customers and partners.

Developing Processes and Skills to Drive Success With Assurance Projects

Focus on enhancing ways of working, managing complexity and driving efficiency and accuracy, delivering faster time to results at a lower cost and with improved employee experience.

CSPs should look to their S&NA solution vendors for support and recommended best practices for processes, skills and approaches to achieve greater success with S&NA transitions. At the same time, CSPs should focus on the skills required to design the future assurance architecture, data management and closed-loop operations while sourcing tools, solutions and capabilities from vendors. Focus on:

- **Engineering to support software-based solutions:** Evolve engineering functions and skill sets to support the move from a traditional, appliance-based legacy approach to new software-based solutions for network assurance.
- **Bridging silos and working across teams:**
    - Eliminate silos between network and operations and between network domains.
    - Interact with CMO and line of business (LOB) leaders as assurance becomes even more essential to delivering customer value and service offerings through SLAs.
- **Capturing and developing skills in a shifting workforce:**
    - Include no-code/low-code platforms to accelerate technology adoption and support citizen developers and business technologists.
    - Capture processes from experienced engineers to replicate in automation processes (such as managing skill loss from the retiring workforce)
    - Select vendors that support the capture of the knowledge of retiring experts into automation processes (such as through supervised or reinforcement machine learning [ML] and guided policy creation and with a roadmap for use of generative AI).
- **Enhancing usability and total experience (TX):**
    - Seek solutions that offer good user interface (UI) with out-of-box functionality, and the ability to custom-organize dashboards for different roles across network engineering, operations, marketing and customer care.
    - Drive TX by linking experiences across user, employee, customer and multiexperience, and provide tools optimized to help employees have better experiences while improving CX. Examples include predictive, proactive notifications of degradations that will negatively affect customers and AI/ML for faster root cause analysis and next best action recommendations, thus improving the experience of both employees and customers.

Evidence

This research is based on 20 CSP OSS S&NA supplier responses to a detailed survey conducted in the first half of 2023. Information was also gathered during briefings by some suppliers and additional companies in the S&NA or service and network testing solution market or other adjacent functionalities. Insights and feedback from inquiries and regular interactions with CSPs were gathered over the past year.

Recommended by the Author

Some documents may not be available as part of your current Gartner subscription.

Market Guide for CSP Service and Network Assurance Solutions

Objectives and Principles for Assurance Architecture Evolution in CSPs

Market Guide for AI Offerings in CSP Network Operations

Market Guide for CSP Service Design and Orchestration Solutions

Use-Case Prism: Generative AI for CSPs