Open Assurance: a blueprint for **data-driven service assurance**

Capgemini

Content

Introduction

Great customer experience is a critical differentiator in the telecommunications market, with quality of experience (user satisfaction both objectively and subjectively) often cited in the top reasons for consumers to change telecom operators.[1][2][3][4]

Service Assurance provides the capabilities that monitor and assure the quality of the service delivered to customers. It is a key factor in delivering a high quality of experience and thus a strong differentiator. Service Assurance is part of the wider Operational Support System (OSS) domain, which also includes the tooling used to plan infrastructure and service expansion, monitor infrastructures, provision new services, and maintain a record of what is deployed.

Given the importance of delivering a high-quality service for customers, Service Assurance is hugely important to CSPs and a whole sector has developed to provide tools to support it. Unfortunately, the existing landscape is often a disparate collection made up of solutions provided by NEPs, often linked to specific technologies, specialized COTS platforms, many of them with proprietary foundations, and internal developments rarely aligned with industry standards.

As a result, CSPs are struggling to provide the high level of quality of experience demanded by customers and, as a consequence, are turning to consolidation and modernization of their OSS estate to drive improvements.

In this paper, we introduce a data-centric approach for the modernization of your Service Assurance domain, defining initial steps that lay the foundations for its wider transformation. You will:

- **Learn about the key challenges and key drivers of modern Service Assurance.**
- **Understand Capgemini's blueprint for Open Assurance as a data-driven approach.**
- **Prepare to integrate Open Assurance in a practical, low-risk manner into your existing OSS.**

[1] Cost is the main reason Americans switch phone carriers. Why else do they jump ship?, from https://today.yougov.com/topics/technology/articles-reports/2021/03/23/americans-switch-phone-carriers

[2] Why do customers switch mobile phone carriers, from https://www.huffpost.com/entry/why-do-consumers-switch-m_b_6525492

[3] The top five reasons people leave their broadband provider, from https://www.which.co.uk/news/article/the-top-five-reasons-people-leave-their-broadband-provider-a91xp8b646hk

[4] Broadband decisions: What drives consumers to switch – or stick with – their broadband Internet provider, from https://docs.fcc.gov/public/attachments/DOC-303264A1.pdf

Key challenges

Here are the **key challenges of today's OSS that we commonly identify in the Service Assurance domain:**

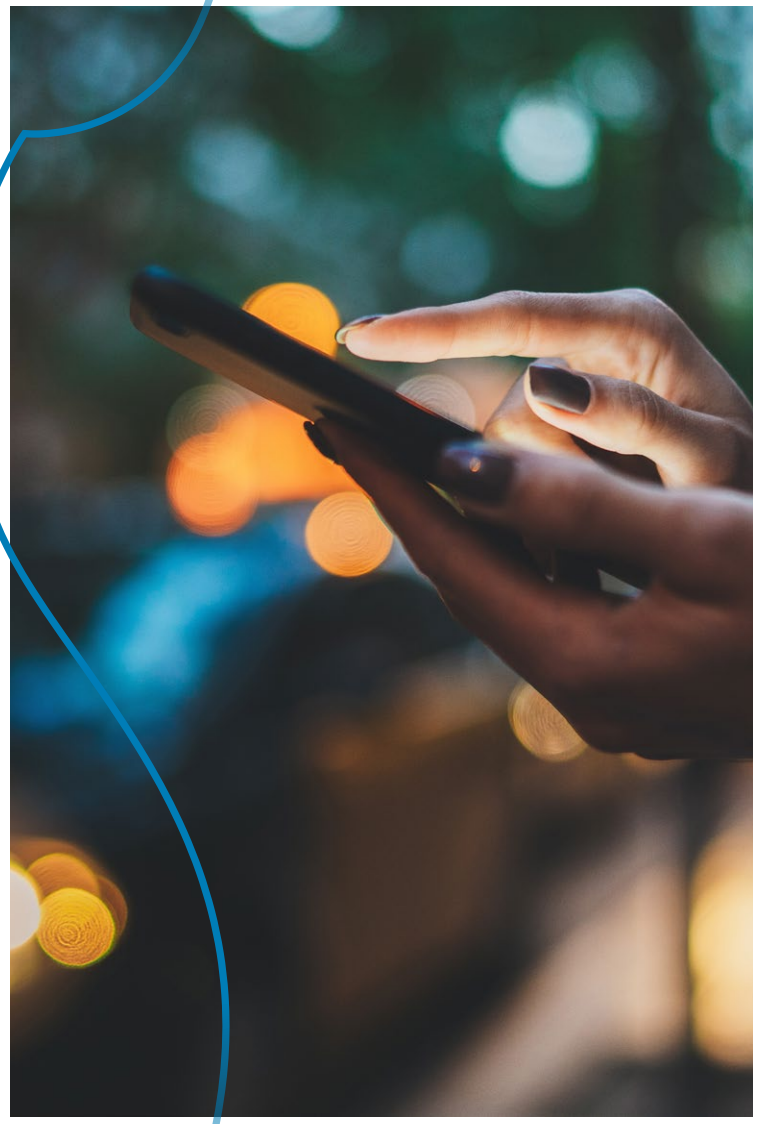
- **Data is owned by vendors,** inside COTS with proprietary models, is not based on standards, and is difficult to access, normalize, and propagate – thus challenging to use outside of the capabilities allowed by vendors.
- **Operations are siloed** with mostly manual orchestration; automation and self-healing are difficult to introduce.
- **Data is siloed –** combining data from several applications is difficult and getting an end-to-end view of quality of experience is nearly impossible without adding deep human expertise.
- **There is difficulty in creating new analytics/AI models,** as you need specialized telco data analytics skills that are relatively rare in the market, and relevant data is not readily accessible. In addition, most vendors want to keep their analytics/AI model as non-shareable IPR.
- **Data quality is low,** data semantics are not well documented, and inconsistencies are widespread – lacking any possibility of global alignment.
- **End-to-end visibility** across layers is weak, especially in a cloud-native world, including, e.g., hardware, virtualized resources, services, and customer layers.

New demands on Service Assurance

At the same time, new demands are being made on Service Assurance. First and foremost, improving quality of experience is critical, as modern society increasingly depends on communications services, and their full availability is taken for granted. Understanding and improving quality of experience requires at least four capabilities that can be challenging to the existing OSS, as they need extensive data collection and analysis:

- The collection of relevant and exhaustive data is needed to understand the service, as perceived by the user and not just the technical quality of service (measurement of the overall performance of a service). For instance, jitter on data packets might be a problem or not depending on your video usage.
- There needs to be rapid identification and resolution of quality problems and incidents, preferably with a high degree of automation to reduce MTTR and drive down costs. For instance, sending technicians should be a last option, in the rare cases where automated remediation is not possible.
- It is necessary to proactively and appropriately inform and provide visibility to customers in case of issues and offer them troubleshooting and diagnostic tools in order to improve client engagement. Getting information from Twitter, and nothing from your CSP, on a collective incident that is affecting you is not acceptable!
- It is important to identify trends and signals precursors for customer impacting events, anticipating problems, and solving them before any negative customer experience.

CSPs also have internal needs to **optimize the use of their scarce resources, notably their personnel**. Data Analytics and AI can drive automation, especially of routine tasks – identifying specific conditions, reacting and correcting, informing customers and users, and asking for human intervention only in more complex cases. Automation lowers the need for human Level 1 monitoring and allows expertise to be focused on the more complex issues, in addition to process setup and tuning, and change management. But **such automation can only be deployed with the availability of high-quality data and flexible orchestration capabilities** together with suitably trained/skilled resources with skills in AI, ML industrialization, and data-driven transformation.



A blueprint for Open Assurance

Open Assurance makes the critical data open and at the heart of service assurance as a common data fabric, notably including technology, real-time and historical status, relationships, and service mappings. This liberates data from the control of the traditional COTS vendors, gives end-to-end visibility of customer service health, and provides the foundational capability needed for the introduction of automated fault remediation – thus enabling the delivery of improved quality of experience and optimized planning.

The diagram below illustrates the Open Assurance blueprint.

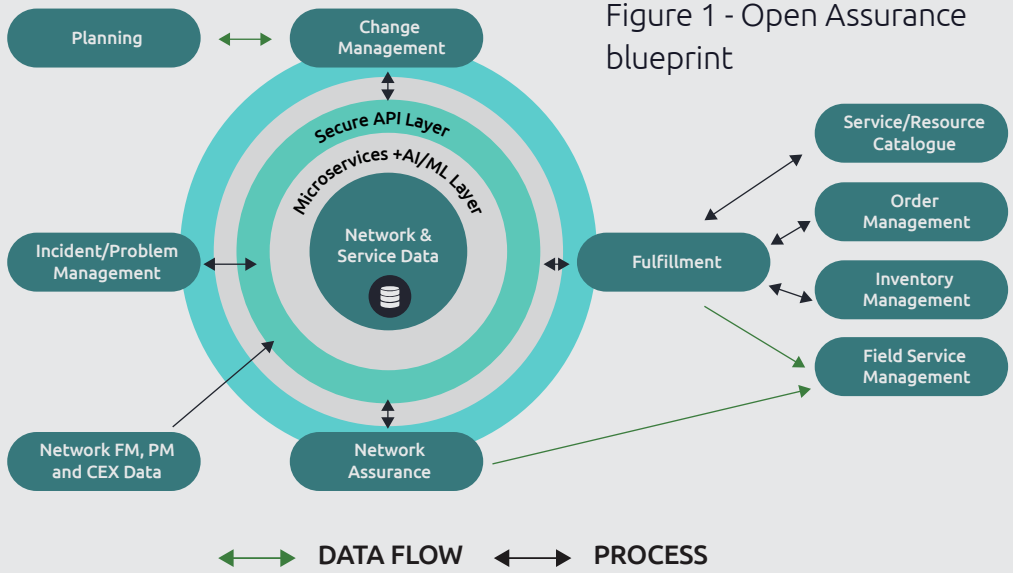


Figure 1 - Open Assurance blueprint

We recommend that the blueprint, its data flows, data repository, data models, microservices, AI/ML layer, and secure API are implemented using an open architecture, owned and controlled by the CSP and providing open access to the data and the associated services, based, where available, on TM Forum Assurance Open APIs, enabling access from all external systems.

We recommend that this capability be cloud based to deliver the required level of agility, performance, and scalability, as well as providing access to the rich collection of data exploration and AI models available on cloud platforms.

This approach enables the continued use of COTS and NEP solutions, thanks to integration via a common data fabric, while enabling the development of additional capabilities using a microservices layer, which includes access to AI models.

An example of a microservice that we would recommend building would be a service that deals with auto-remediation of faults or performance degradations. The assumption is that the legacy system does not know how to remediate a service problem in a specific environment. The offered service would enable the originating system to enter specific details on the fault, including device ID and type of fault, and the microservice then deals with initiating the appropriate process to complete a remediation task. When complete, the service reports back to the originating system. In such a way, automation is built outside of the traditional, closed COTS platforms. We can gradually build a centralized, contextualized, and actionable smart operational data layer to exploit both machine intelligence (AI and ML) models and catalogue-driven case orchestration templates, providing an intelligent, real-time, contextual analytics central brain enabling closed-loop automation.

Transitioning to Open Assurance

While the blueprint illustrates the recommended target state, we appreciate that CSPs cannot simply move from the existing operational environment to this new blueprint overnight. An approach that enables transition while minimizing risk is imperative.
Figure 2 illustrates the proposed transition process at a high level.

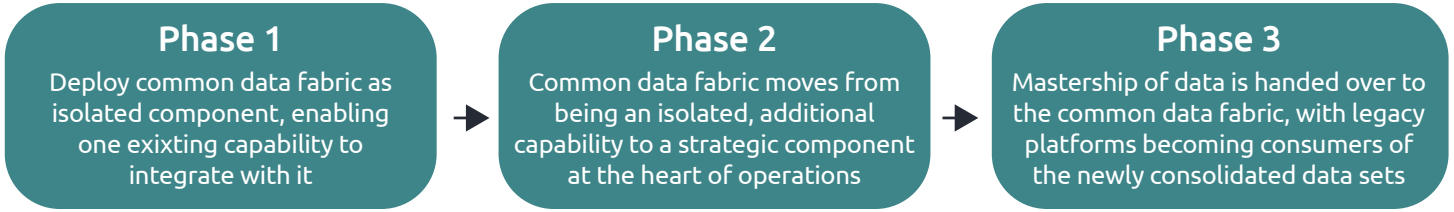


Figure 2 – end-to-end transition process

Phase 1 sees the deployment of the common data fabric as an isolated new component. An existing platform that can make the best use of this new capability is then selected for integration, which involves pushing a version of its own data into the new common data fabric and/or collecting data in real time directly from network sources. The critical point at this stage is that the introduction of the new common data fabric does not impact the normal operational working of the selected platform. During this phase, the analytics team can start to experiment and create additional insights from the analytics and, where appropriate, offer these back to the original system for inclusion in its operation via data-enabled microservices.

Additionally, those insights can be made available via new, dedicated UI, such as dashboards, reports, and ad hoc exploration tools. This phase enables a progressive delivery of the first capabilities, allowing exploration and confidence to be built in the approach while liberating from some of the constraints of legacy systems – those constraints can be latency (moving to real time), storage capacity (from a few days/weeks to months of historical data), data model (from a proprietary, non-documented model to an open, standard-based data model), exploration capacity (from limited compute power to wide elasticity), availability of AI tools (platform-based), and more.

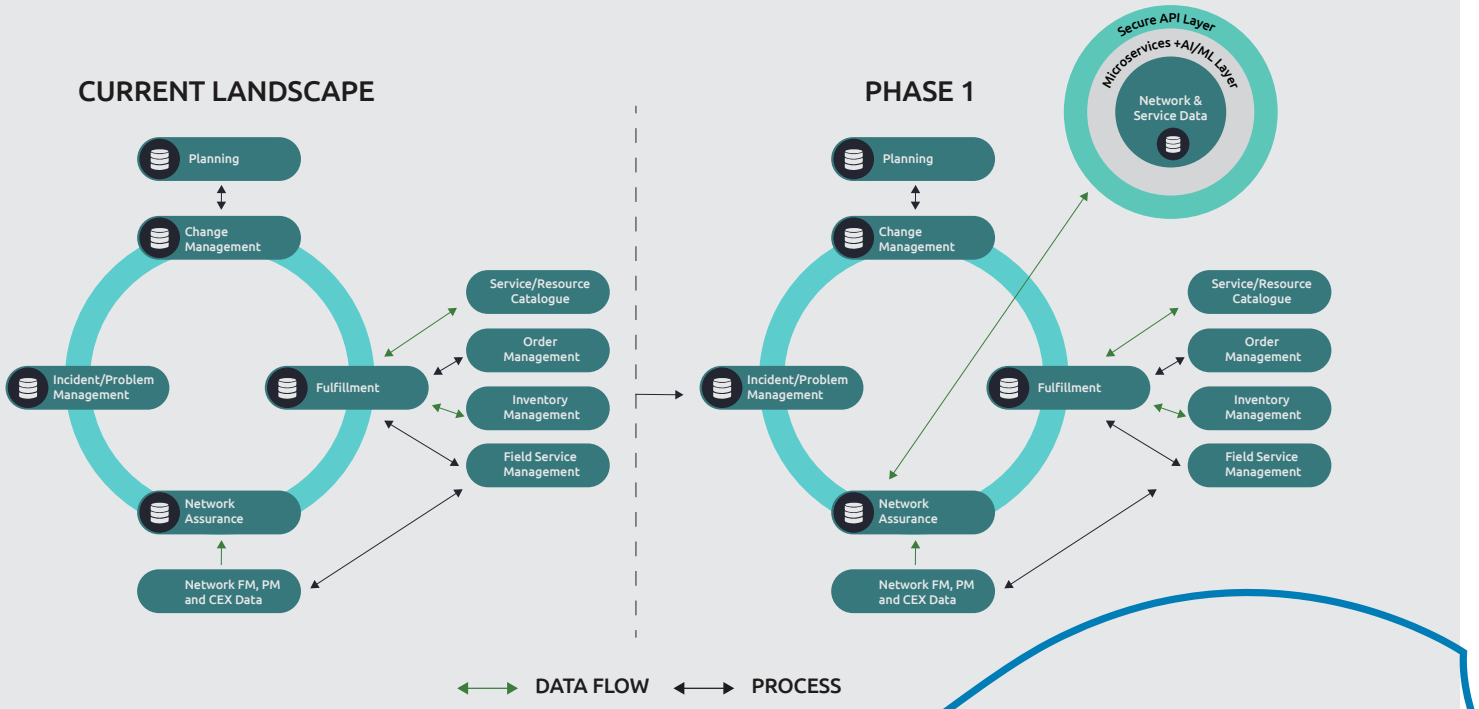


Figure 3 – Transition to blueprint – Phase 1

Example: a major European CSP is setting up a new data platform for mobile tower telemetry on a cloud platform. This platform will at first enable real-time dashboard production and data exploration, and will then progressively provide analytics insights back to operational applications.

Once confidence has been established in the common data fabric and the analytics team is using it to create actionable insights, it is time to move to Phase 2 of the transition. This sees the new common data fabric move from being an isolated, additional capability to becoming a strategic component at the heart of the operation. During this phase, we provide all the appropriate data from the various capabilities to the common data fabric and start to develop additional insights from that data, which can either be fed back into those individual systems to augment their own processes or for use in other systems – again via microservices. During this phase, the existing platforms are still seen as the masters of the data they hold, with the data fabric being a consumer.

Example: a major broadband operator in the US has set up a real-time data fabric, processing CPE telemetry, network alarms, and incident tickets to derive insights available to network operations, technical support, and customer support.

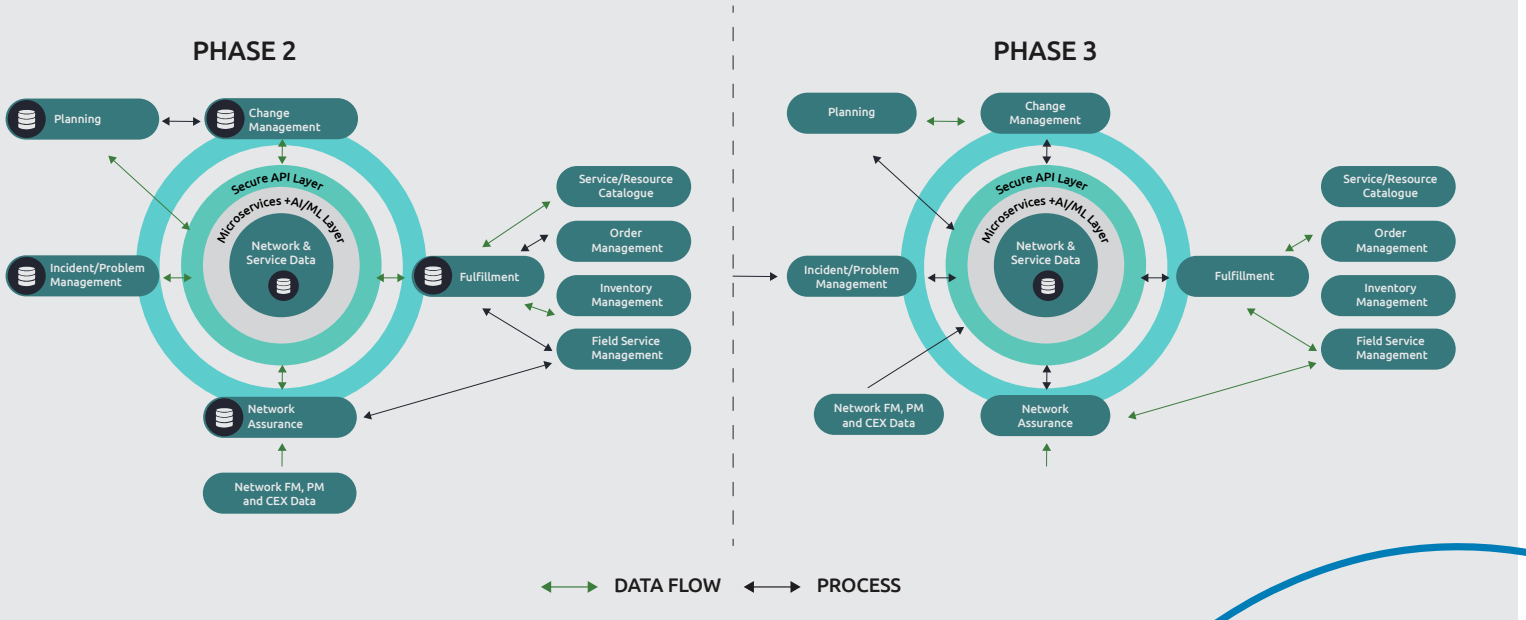


Figure 4 – Open Assurance blueprint

Finally, once all the systems have provided the appropriate data to the common data fabric, as part of the final Phase 3 of the transition, mastership of that data is handed over to the common data fabric and the legacy platforms become consumers of the newly consolidated data sets, as needed. It should also be noted that, at this stage, event and performance data will be redirected and consumed by the common data fabric first and then passed out to the Fault and Performance Management systems. This approach enables the CSP to develop their own real-time FM and PM analytics, if desired, alongside, or instead of, the traditional vendor products.

While it is easy to propose new architectures and approaches, it is quite different to actually implement them. We have been working with a major CSP client on this very issue as described in the next section.

Case study: a US broadband operator

We have used this blueprint with one of our US clients, a broadband operator, to implement a platform providing service assurance automation.

Our client has started their journey to Open Assurance by implementing a whole set of Service Assurance functions for broadband services on a new common data fabric. This includes analysis of network topology, CPE telemetry, network faults and incidents, and technical trouble tickets.

It exposes the new services offers, via open APIs, to the customer service and technical support teams. Figure 5 on the next page illustrates our client's deployment; as you will see, it is effectively a Phase 2 deployment.

Identify collective incidents, and improve service call handling by deflecting

25%

of customer calls.

This approach has allowed our client to reduce truck rolls by

30%

Improve fault detection accuracy by

30%

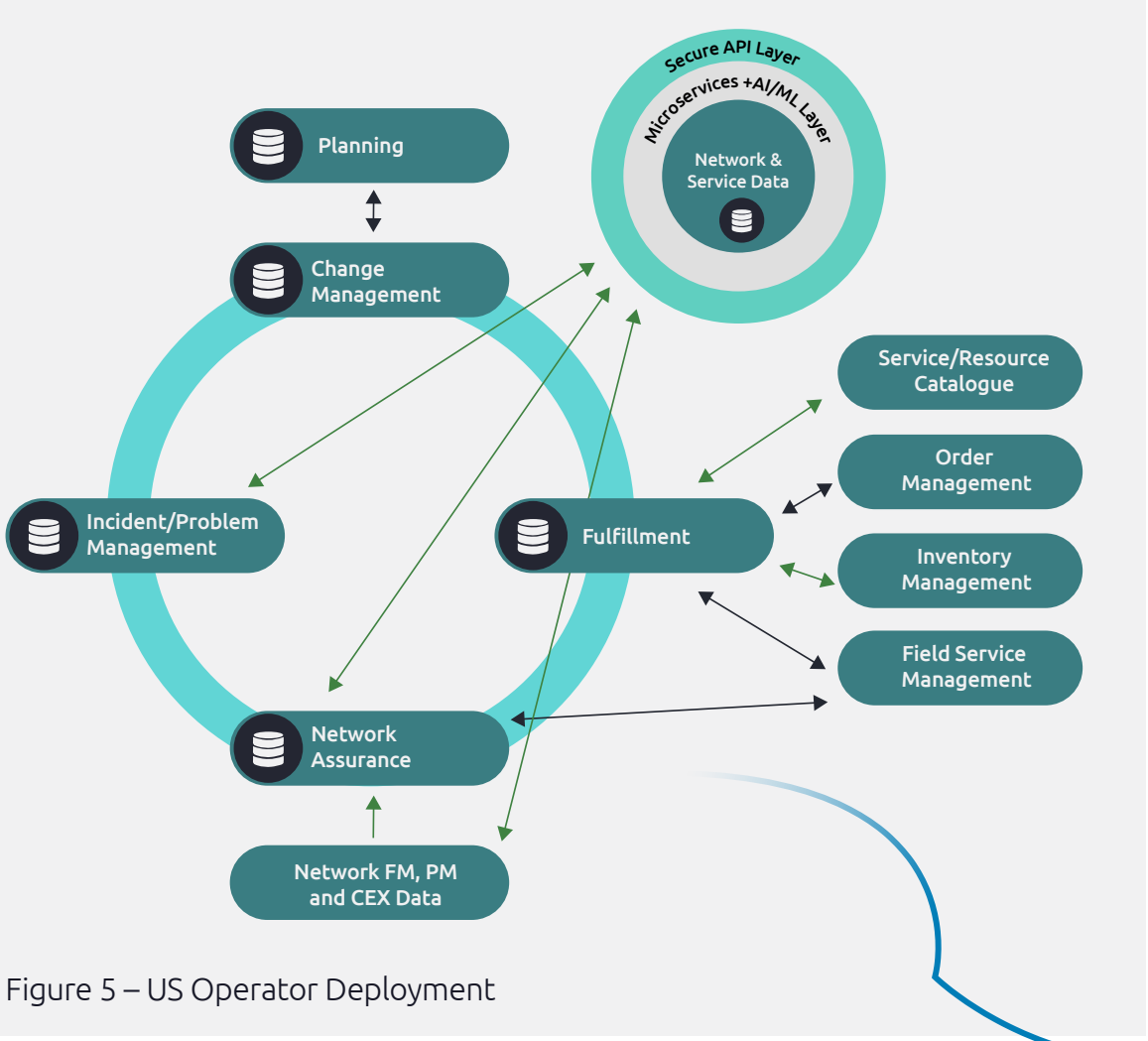
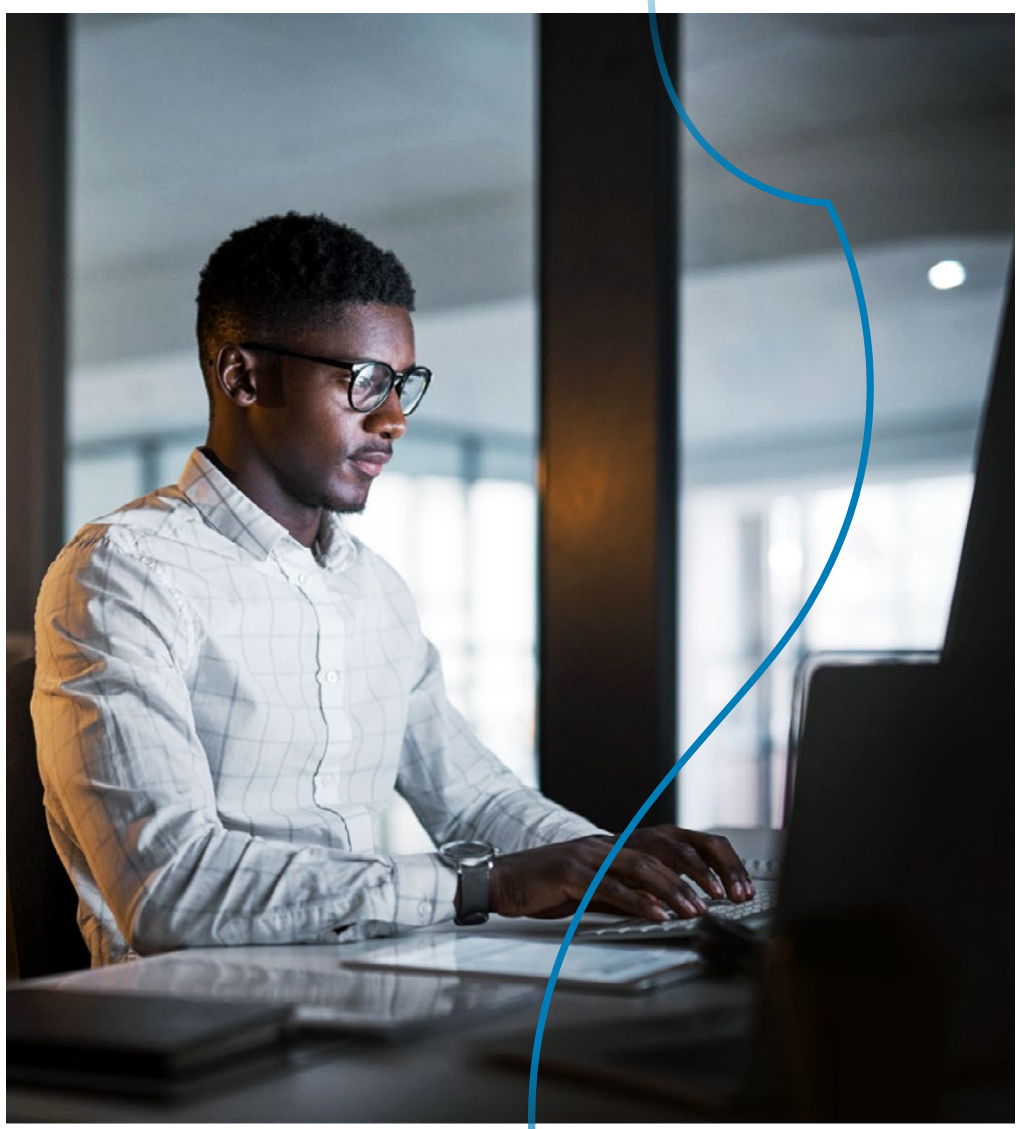


Figure 5 – US Operator Deployment

Based on open data analytics technologies, this common data fabric enables the collection and processing of telemetry information from CPEs – modems, set-top boxes, routers, and home equipment – and combines this with network alarms and trouble tickets in real time to provide services to the different operational domains responsible for managing quality of experience, including call handling, customer support, and technician dispatch. The platform is fully controlled by our client and is evolving to cover new needs, adapt to new network technologies, and add new data for better insights.

Business capabilities

- **Full access to home health for CSRs.**
- **Proactive customer information in case of individual or collective incident.**
- **Assisted diagnosis by technical support with root cause analysis.**
- **Advanced identification of fault conditions that might lead to service disruption before experienced by customers.**



Key characteristics

- Data-driven automation architecture, owned and controlled by the CSP, that makes use of the expertise embedded in the best-of-breed COTS components, while creating additional capabilities to drive end-to-end quality of experience improvements.
- A use case-centric approach, allowing the delivery of new capabilities incrementally, evolving with the needs of the CSP, while progressively building a platform mutualizing data and algorithms for a variety of uses.
- Provides an environment that supports a highly agile approach to the development of services and other capabilities.
- Modular and open as far as possible to simplify integration and optimize access to both the CSP and its SIs who have a key role in building out additional services.
- Provides an end-to-end "holistic assurance" capability that goes beyond traditional fault and performance management on existing infrastructures, which also aids the planning and development of future services, as well as improvements in quality of experience.

Conclusion

To be useful and fulfill its promises, data needs to be liberated, accessible, and understood – and it is not today in most legacy OSS architectures. CSPs can start implementing an Open Assurance framework today to bring the full benefits of modern AI and analytics. They can then get a deeper, more holistic understanding of their operations and bring information to bear more rapidly. They can build better closed-loop automation for more autonomous networks[5], thus simultaneously enabling higher efficiency and higher quality of service.

High investment costs in new network technologies and threatened margins make it necessary to optimize operations costs while satisfying strong demands for quality from customers. CSPs need to transform their operations in general, and Service Assurance more specifically. We have shown how Open Assurance can be implemented in an agile, iterative way into legacy OSSs, morphing them into a more agile, data-driven OSS supporting a higher level of network autonomy, while avoiding the risks associated with massive upheavals.

Let's do it together!

[5] Autonomous networks: exploring the evolution from level 0 to level 5, TM Forum, https://inform.tmforum.org/research-and-analysis/reports/autonomous-networks-exploring-the-evolution-from-level-0-to-level-5/

About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of over 325,000 team members more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2021 global revenues of €18 billion.

Get the Future You Want | www.capgemini.com

Contact our experts:

GIORGIO DI CAPUA
Telco & Media Presales Lead,
Capgemini

IAN MIDDLETON
Telco Architecture Lead,
Capgemini Invent

YANNICK MARTEL
Data & AI Lead Telecom industry,
Capgemini