The journey to the cloud with 5G

Communication service providers (CSPs) are already rolling out 5G NSA ultra-broadband services for their customers, but it is Industry 4.0 and enterprise verticals that promise the biggest potential for new revenues. This new market opportunity will require cloud-native 5G standalone (SA) to both meet enterprise requirements, such as low-latency, massive IoT support and network slicing, and to reduce the operational costs associated with tailoring solutions to the specific needs of large enterprise clients.

Reducing operational costs will require CSPs to embrace DevOps-style methodologies adapted to the telco environment with automation playing a much bigger role than today. Along with this organizational shift, CSPs will have to transform technologically, embracing containerized network functions (CNFs), designing their core and edge cloud infrastructure and even redesigning their transport networks to support 5G SA. With this complexity also comes new issues around securing the network.

In this white paper, we look at the CSP journey to 5G and cloud-native and introduce our methodology for engaging with CSPs on the transition and the issues they have to consider. As one of the few vendors with an end-to-end 5G portfolio, we share our insights across all domains and provide valuable insights on the transformation process based on our global advanced consulting engagements with a wide range of operators from greenfields to global incumbents.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Enterprise services</td>
<td>3</td>
</tr>
<tr>
<td>Other 5G drivers</td>
<td>4</td>
</tr>
<tr>
<td>The 5G operational transformation</td>
<td>4</td>
</tr>
<tr>
<td>Telco cloud organization</td>
<td>5</td>
</tr>
<tr>
<td>Cloud transformation operations consulting</td>
<td>6</td>
</tr>
<tr>
<td>Design and build</td>
<td>6</td>
</tr>
<tr>
<td>The 5G technology transformation</td>
<td>8</td>
</tr>
<tr>
<td>VNFs or CNFs?</td>
<td>8</td>
</tr>
<tr>
<td>Cloud architecture</td>
<td>9</td>
</tr>
<tr>
<td>Cloud transformation technology consulting</td>
<td>9</td>
</tr>
<tr>
<td>5G security in the cloud</td>
<td>10</td>
</tr>
<tr>
<td>Security operations</td>
<td>11</td>
</tr>
<tr>
<td>Cloud transformation security consulting</td>
<td>11</td>
</tr>
<tr>
<td>Why Nokia?</td>
<td>12</td>
</tr>
</tbody>
</table>
Introduction

With much fanfare, the mobile networking industry is currently in the process of rolling out 5G. New 5G-enabled smartphones will be big items in the coming holiday season. Most communications service providers (CSPs) will be heavily marketing new Apple and Samsung handsets in a head-to-head competition for the lucrative upgrade market, and it will seem that 5G has arrived.

Despite the fanfare, this first 5G round is really the continuation of the old paradigm with predominantly the non-standalone (NSA) version being deployed. As with previous generations, it is touted as offering more bandwidth and speed to support the latest round of consumer applications. Just as we moved previously from loading image-rich web pages with 3G to listening to and watching streaming media with 4G/LTE, 5G NSA is promising higher-definition video and augmented and virtual reality (AR/VR) applications.

Mobile operators understand that this is just the first step, however, and they need to make the next step to 5G standalone (SA) for reasons other than keeping their consumers supplied with more and more bandwidth. They are struggling to generate enough additional revenue in the consumer segment to justify the investments they are having to make. Competition from alternate providers is eroding margins. Growing revenues in today’s markets means entering new markets, such as specific enterprise verticals, and creating custom solutions for individual large customers.

This is a different operational model for CSPs that are used to mass market consumer offerings. It will require greater agility and the need to develop and integrate faster. They will need to reduce the costs associated with running their networks as well as the CAPEX demands of building out capacity. Cloud-native 5G SA promises to deliver on both those fronts, but it will require considerable effort to implement its cloud-native architecture and realize the benefits of its flexibility, faster time to market and improved automation.

Enterprise services

With the erosion of profits on the consumer side of their businesses, most CSPs currently have their sights set on the enterprise market for new 5G services. The adoption of Industry 4.0 technologies such as automation, IoT and AI are driving a productivity revolution. Traditional infrastructure industries such as power utilities, mining, logistics, manufacturing and transportation have largely resisted the digital trend until recently. They are now embracing the digital transformation of their operational technology and need a robust wireless solution to support their use cases. This represents a huge and profitable market for CSPs.

The prospect of billions of IoT sensors and autonomous vehicles such as ore trucks and robots is driving industries to look for wireless solutions that are superior to existing alternatives. Wi-Fi, for example, doesn’t have the deterministic performance and reliability required, nor does it support mobility beyond a walking pace. On the IoT front, there have been multiple flavors of low-power wide area (LPWA) technologies introduced, but these constitute yet one more specialized overlay network to deploy and maintain.

Although 5G can coexist with any of these technologies, one of the big drivers for enterprises is the possibility that it can consolidate all existing operational technology (OT) networks onto one, doing everything from LPWA and private radio to high-bandwidth mmWave and ultra-reliable low-latency communications (URLLC) for precise automation requirements. 5G network slicing is also expected to be a game-changer for many industries, allowing private wireless services to be tailored to the precise needs of each use case. All these capabilities mean a wholesale shift to cloud-native 5G SA.
Other 5G drivers

On the consumer front, the much-touted mmWave frequencies (24–48 GHz) will require more than an upgrade to 5G New Radio (NR) for existing macro cells because of the severe signal attenuation from which they suffer (for this reason, the majority of new 5G NSA deployments use low-band 5G at 600 and 850 MHz). They will require an entirely different approach using small cells to focus the coverage in dense urban areas where there are a lot of users looking for very high bandwidth. Small cells will also be used extensively in enterprise deployments for delivering very high bandwidth and low latencies.

Scaling their networks and operations to meet this new demand from enterprises and dense urban coverage is expensive based on the old hardware paradigm. Whereas, going cloud-native will make scaling capacity a simple matter of spinning up new cloud-native network functions in the cloud. On the operational front, CSPs can move to a more automated deployment model using continuous integration and continuous deployment processes. This will greatly reduce their operational costs, improve reliability and speed time to market for new features and services.

One of the key aspects of 5G is its overall flexibility. It can use a wide range of spectrum and can adjust to different operational demands, from massive IoT (a million sensors per square mile) to very low latency (<1 ms) communications. And the core resources to support these very different requirements are shared on a single cloud infrastructure, which optimizes that investment no matter what usage pattern develops over time. Capacity to handle video streaming and virtual reality gaming on the weekend, for instance, is also available for industrial use during the week.

The move to cloud-native 5G, in other words, promises to provide CSPs with a connectivity platform to provide mission-critical and business-critical services to enterprises and other organizations, such as public safety and smart cities, and meet the demand for new ultra-broadband services for consumers. It sounds straightforward, nonetheless, there are a lot of moving parts to this transition. We will look at the operational, technology and security aspects of the 5G journey in the following sections.

The 5G operational transformation

The reliability, flexibility and scalability of 5G also has a flip side, which is complexity. Without automation, the 5G network would be impractical to run manually. It would certainly be too expensive. For this reason, automation and orchestration are baked into the design of 5G.

The operating environment for 5G networks is, nonetheless, quite complex, especially when most CSPs will still be running legacy infrastructure alongside it for a long time to come. There are multiple technologies involved, such as bare metal, virtual machines and containers, multiple cloud environments — private, public and hybrid — and multiple vendors working at different layers in the system with both proprietary and open-source solutions.

The operator of a 5G network faces multiple challenges. For example, they must minimize downtime by preventing failures, instantly identifying root causes and restoring services immediately. At the same time, they must re-align the organization and its teams to speed up development and deployment. This requires reducing the time needed to build new functionality and integrate it into production environments for faster launch of fixes, features and services. The increased pace of development, deployment and integration plus the requirement to scale rapidly means automation wherever possible is required to keep up.
**Telco cloud organization**

A cloud operating model is designed to meet these challenges by integrating the traditional departments found in most CSPs, such as Business, Engineering, IT, Value Added Services and Operations and Maintenance, into horizontal “as-a-service” slices. At the bottom of the stack, infrastructure-as-a-service provides lifecycle management, virtual compute and storage resources and the software-defined network elements. On top of this layer, platform-as-a-service provides lifecycle management of the virtual functions, whether virtual machine (VM)-based network functions (VNFs) or container-based network functions (CNFs). It also provides the various software components and development of new innovative features and services. Network-as-a-service provides lifecycle management for services and manages the customer’s experience and provides customer self-management.

Figure 1. Target future mode of operations

To move to this cloud-native “as-a-service” operating model is complex and requires careful planning if the CSP is going to realize business value in making the transformation. It is essential for the CSP to identify what the end goal or target operating model for the cloud will be before starting. It is rarely the case that a CSP will move immediately to an advanced cloud-native operational state, especially given that many of the changes require new skills and behaviors, which take time to develop.
Cloud transformation operations consulting

In our consultations with many CSP customers, we start by defining the business requirements for their cloud operations. We discover the current mode of operations, identify the new set of operational capabilities, define the target operating model and then assess the gaps and priorities so that we can develop a roadmap for the transformation. We use Nokia’s Advanced Telecom Operating Model (ATOM) framework to bring together several industry standards to define the target operating model so that CSPs can reap the benefits of cloud via efficient cloud operations. This includes assessment and planning for the cloud platform, processes, performance KPIs, skills and competencies, as well as the business value the CSP hopes to realize.

Design and build

To design and build the new operating model or future mode of operations (FMO), we apply the results from our ATOM framework to design the FMO, the new advanced operational capabilities to be supported in the new organization model, KPIs and tools. We identify the new process and skills gaps and how best to enable current employees through upskilling in some cases and reskilling in others. Beyond training, it is critical to reinforce new skills acquisition with proper incentives by aligning processes and KPIs to support personnel and teams to make the transition. The transition plan should also identify quick wins for personnel to consolidate early buy-in to the goals of the transformation.

The introduction of DevOps is one of the biggest organizational shifts for most CSPs. Originating from the original “goldrush” mentality of the early internet, webscale companies put a higher priority on capturing market share with new cloud services than ensuring quality upon launch. They developed a process for iterating quickly, failing fast, and fixing even faster. DevOps crucially requires the operations team and the development team to closely collaborate so that the development team arrives more quickly at a production-ready product through continuous integration and continuous delivery (CI/CD).

In the more complex telco environment, the final deployment environments are less homogenous than in the webscale space given the legacy infrastructure present in most CSPs. Thus, deployment often means delivering new software into multiple operating environments, which calls for more focus on delivery operations. This requires greater focus on automation to ensure that CSPs can achieve the benefits of the DevOps approach. Operators focusing on a Cloud Operations Services Catalogue will have a leading edge in implementing a DevOps based operations lifecycle over other operators.

One of the ways to reinforce the value of the transformation is to introduce automation methodically. Focus on those aspects of the operation that no one will miss performing or those that concern entirely new processes and functions un-related to previous operations. Honor the acquired expertise of valued personnel by recognizing it in the automation workflow so that automation augments their decision making while preserving their self-worth. Being part of the design and build process is another important way to build buy-in.

Our process for carrying out this transformation is designed to work at multiple levels within the CSP organization to ensure support from bottom to top. Strategic consultation, planning and goal setting ensure early executive buy-in, while process design and delivery engage the operational teams early to
give them a tangible stake in the result. Throughout the execution of the plan, it is critical to communicate frequently. Once the principal initiatives have been identified and prioritized in the transformation roadmap, the change management communication plan is a key deliverable.

To ensure that the CSP achieves its business value realization (BVR) targets, it is important to begin by baselining the existing performance of the business against the identified KPIs, wherever possible. Then it is important to track those KPIs over time, doing regular analysis to identify where there is lack of progress and design programs to address those areas. The period for analysis depends entirely on the function and level of detail involved. For implementing DevOps practices, it could be weekly or monthly review of dashboards, whereas for higher level goals such as skills development, it could be every four to six months.

Seizing the cloud opportunity in Asia-Pacific

This tier-1 service provider was challenged to move to cloud-native as part of their embrace of 5G. In our initial discovery, they identified the need for new cloud skills, organization structure, tools and processes. They were concerned that their incentives were not aligned properly with the new goals of the organization, which were to harness the cloud and become more agile and efficient. Agile development methodologies (e.g., DevOps and CI/CD) were clearly needed, but they were unsure how to introduce them and automate their delivery processes.

Nokia engaged with them using our ATOM methodology to define their target operating model. We captured their then-current mode of operation for both existing virtualized and legacy infrastructure, networks and services. We worked with them to design their future mode of operation covering the four Ps: process, people, platform and performance. Our gap analysis resulted in roadmaps for building new processes and organizations, with KPIs for every stage of the journey. Skills deficiencies were identified, and training programs designed. Finally, we developed a follow-up business value realization program for assessing the success of the new operating model.

They successfully launched their journey to the cloud and continue to work closely with Nokia as a trusted partner as they realize greater efficiencies, agility and launch new services for their customers.
The 5G technology transformation

The move to cloud sounds primarily like a shift in technology but, as we’ve discussed, operations, organization and skills are probably more important in the final analysis. The technology issues are, nonetheless, crucial.

VNFs or CNFs?

The move to cloud-native began a decade or more ago with the move to virtual network functions (VNFs). Most VNFs were originally realized on virtual machines (VMs) dedicated to each VNF. This made virtualized functions easier to integrate with legacy equipment, since they followed the hardware paradigm more closely, but they didn’t fully realize the benefits of a virtualized approach. Virtual compute and storage resources ended up being dedicated to the network function and couldn’t be dynamically used for other tasks.

Cloud-native introduced a more disaggregated approach, where microservices were deployed in containers and linked together to create network functions. Containerized network functions (CNFs) are made available in an environment like Docker, which provides some of the common operating system functions. This means the CNFs are lighter and faster to load and virtual resources can quickly be assigned and reassigned to other microservices, making the utilization of the underlying compute, storage and network resources more efficient. The lifecycle of CNFs is managed by Kubernetes, which is an open-source orchestration platform for containers.

Whether this additional efficiency is realized in practice depends a great deal on the design of the network and service being supported. Some services have a statistically stable demand profile where the move to containerized microservices doesn’t yield a great deal of efficiency and a VNF approach is fine. 5G supports such a wide range of services and use cases that the presumption is the CNF approach will be best suited to enabling that flexibility. However, a CSP’s organization may already be very familiar with operating VNF environments, and it may make more sense organizationally to continue to leverage that familiarity and introduce CNFs more slowly.

Figure 3. The path to cloud-native
Cloud architecture

Cloud configurations are many and again will be highly dependent on the customer. Tier 1 operator’s typically have their own private clouds and will at best turn to public clouds for non-network workloads or where they lack resources. For instance, where they need to provide edge cloud functionality to an industrial client’s private wireless service, they might turn to a local collocation provider for edge cloud resources. Whereas a greenfield operator is more likely to go directly to the public cloud.

For incumbents with legacy infrastructure that includes, for instance, central offices, they may make the decision to leverage that infrastructure to provide edge cloud services to themselves and others. As 5G consolidates different services, including fixed access, it will inevitably be the case that different silos have been operating their own data centers that can now be combined.

The design of the cloud architecture will thus be unique for each CSP and will be determined by cost efficiencies, geographical location of their enterprise customers, and what kinds of applications and use cases they need to support. Automation use cases, for instance, will require edge cloud support for low latencies. A mining customer might need far-edge support, whereas an auto manufacturer needs support from the metro edge.

For mobile consumer services, there are additional considerations for cloud RAN. CSPs will need to support their cloud RAN data centers with transport trunks, which will determine where they can locate them and how they architect their backhaul network. Do they have sufficient bandwidth to do the processing centrally, or will it be more efficient to distribute some 5G core functions to the edge to shorten fiber spans? This could enable, for instance, backhauling the 5G small cell radios with the latest high-speed versions of PON.

There are a further set of issues that affect the choice of cloud architecture. Local regulations such as the European Union’s GDPR may favor the use of private clouds, for instance. To what extent are OSS/BSS partners engaged and how does the CSP want to expose the network to them? As with all technology adoption, there is also the typical issue about whether to go with a fully engineered solution or best of breed?

Cloud transformation technology consulting

In consulting with our CSP clients, the above only begins to capture the range of possible issues. This highlights the need to develop a cloud strategy at the start. What cloud model does the CSP want to target for their transformation? There are business drivers, issues of skills and cloud-native readiness, and the services and customers they want to reach. We work closely with them to assess their existing cloud implementations and then develop a preliminary roadmap.

The design of the actual cloud architecture needs workshopping to hash out details such as plans for automation, DevOps and how extensively the CSP intends to implement containers versus virtualization or bare metal. From this work, we create a candidate cloud architecture and then workshop it again, laying out responsibilities, defining a minimal viable release, creating an implementation plan and identifying risks and mitigations.

Finally, we undertake the cloud migration beginning with a readiness assessment based on a gap analysis comparing the current setup to the target architecture. From this we develop a transformation deck that includes a risk register, a working team environment including tooling, an agreed-upon definition of done, and confirm what constitutes a minimal release. This is all encapsulated in a release and delivery plan.
5G security in the cloud

Security in the 5G era comes with challenges that arise from the increasing complexity of the network, the move to containerization and the distribution of the cloud. At the same time, 3GPP has addressed security in the design of 5G to give it greater flexibility than previous generations. For instance, the authentication framework is now access-agnostic for enhanced subscription privacy. User plane integrity protection has added encryption to make it more robust, and network slicing now has specific authentication and authorization mechanisms.

Despite these and other changes, 5G creates challenges for security design. Encryption is more complex with issues such as encrypting cloud-native databases, rotating encryption keys and where keys are stored. Because of the greater complexity of the cloud-native architecture, there will need to be automated, self-adaptive, intelligent security controls at many layers in the architecture. Network functions that were in dedicated hardware and software units previously, are now disaggregated, container-based microservices that are loosely chained and hosted in a virtualized environment, which greatly expands the attack surface.

That environment, which includes the hypervisor, container platform and orchestration layer, must be sound with robust implementations to ensure security. Yet Kubernetes and other public clouds do not fully understand the layers of security that the telco environment will require. Environments like Docker can be helpful by isolating containers, but this can also be eroded by overly expanding the interconnection of containers resulting in an increased attack surface. Meanwhile, the Cloud Native Compute Foundation (CNCF) has only just begun to analyze the complexities and challenges posed by cloud-native architectures. There is a great deal of work still to be done.

On a positive note, 3GPP has developed new security concepts to deal with service-based architectures, including mutual authentication between network functions and transport layer security for all communications between them. It has also developed an authorization concept to enable granular control of service usage between network functions.

The cloud journey in Europe

This Tier 1 European operator was facing multiple challenges establishing its network function virtualization infrastructure (NFVI). It had issues around the end-to-end ownership of the infrastructure and how to manage its partners and other third-parties as they onboarded new VNFs.

Nokia’s Cloud Transformation consultants proposed a solution, assembling a group representing all the players that was then responsible for end-to-end incremental project design. They developed a commercial model based on outcome-based deliverables and leveraged the best practices and successes of other European operators.

The project successfully established end-to-end responsibility and management for the support of incremental projects. It established clear planning and ownership for performance management, capacity management and future expansions such as 5G. As part of this, they defined KPIs and agreed on schedules, costs, quality and the team of people involved, creating a roadmap for development in 2021 that included migrations, NFVi extensions, upgrades and new hardware.
Security operations

On the operations front, the transition to DevOps means that security concerns will need to move upstream in the development process as well. This will lead to DevSecOps (development, security and operations) and much greater scrutiny of the software supply chain, which has seen a growing number of attacks recently.

Despite new authentication functions, slicing remains somewhat of an operational problem in terms of its demands on security orchestration. Slice security needs increased automation to make it more manageable. Perimeter security needs to become layered so that firewalls can be set up, not just around the entire network, but around individual slices, with much more granular reporting of incidents at the slice level.

The distribution of core network functions from the core to the metro and far edge will require security orchestration, which is not a problem that public cloud operators fully understand. Since the distribution of core functions is dynamic, it is not a case of setting it up and leaving it. The application will automatically cause the core to reconfigure itself in real-time to meet parameters such as latency. Security measures must be orchestrated dynamically to match the distribution of functions, authenticating interactions between core functions and isolating the more exposed perimeter.

Regulatory requirements also need to be orchestrated, such as service control points used for lawful intercept, which now must be dynamically implemented at the container level as voice calls are spun up and down.

Cloud transformation security consulting

We have helped hundreds of CSPs to transform their security systems, which gives us unique insight into what is needed to secure the complexity of the telco environment. We are also one of only two vendors that has an end-to-end 5G security infrastructure.

In our consultations, we begin with a strategic security assessment. This includes a risk assessment, security scan, audit and review of the current and proposed cloud architecture for compliance with your technology and market profile. This leads to a gap analysis between your current and target states. We use this to recommend how best to design protection for your various domains, including the security of both your private and public cloud infrastructure.

This cybersecurity roadmap is used to guide your security transformation and operationalize your 5G cybersecurity framework — an advanced response architecture for rapid, accurate security insights and responses across all your endpoints, networks, cloud services and users. It will ensure that your technology is up to date and that your security processes and policies are aligned with cloud-native technologies.

On the operational front, it will give you full visibility over your deployed base and potential threats you will need to monitor. It will design and build automated processes to ensure that other cloud-native automated functions, such as orchestration are matched by security automations, ensuring the integrity of your DevOps automated deployments. Finally, it will identify potential areas of concern that will require process and technology innovations and the evolution of 3GPP and open-source standards.
Why Nokia?

The journey to cloud-native and 5G services is only beginning with the rollout of 5G NSA services. With flat and declining consumer revenues, CSPs must shift gears as private wireless becomes an important driver of Industry 4.0. This new market will demand a more bespoke, less mass-market approach to delivering services. It will only be cost-effective if the network can become extremely dynamic and flexible in an automated way, which is the promise of 5G.

3GPP has worked closely with industry to engineer features like ultra-reliable low latency, massive IoT support and network slicing to specifically meet the needs of industrial users. Nokia is the world’s leader in providing private wireless networks to industry verticals and understands the dynamics and needs of the Industry 4.0 market. CSPs have an unprecedented opportunity to grow their business into this market and reduce their operational costs at the same time.

In order to make this transition to cloud-native, CSPs will have to re-design their operations, make the technological transition to the cloud and ensure the cybersecurity of their 5G network. All of these are big challenges that will require the help and collaboration of many partners. At Nokia, we have an established track record helping some of the world’s biggest operators to embrace 5G and the cloud.

We are one of the only vendors with an end-to-end 5G portfolio. We have expertise across all domains, as well as an in-depth understanding of legacy telco environments and operations. With over 200 field-proven use cases, we have a wealth of process maps and global best practices to draw from. We can bring valuable insights to your transformation process based on our global transformation practice with a wide range of operators from greenfields to global incumbents.

Our Nokia Bell Labs researchers lead the world in the development of many of the technologies that are part of this evolution, playing key roles on 3GPP working groups in defining the 5G standards. We have one of the only end-to-end security solutions for 5G and we have a demonstrated ability to create technology blueprints for cloud and 5G and work closely with our service teams to help you implement them.

To help you in your cloud transformation journey, Nokia offers a Cloud Transformation Consulting service that puts our experience and expertise at your fingertips. Contact us to find out more.