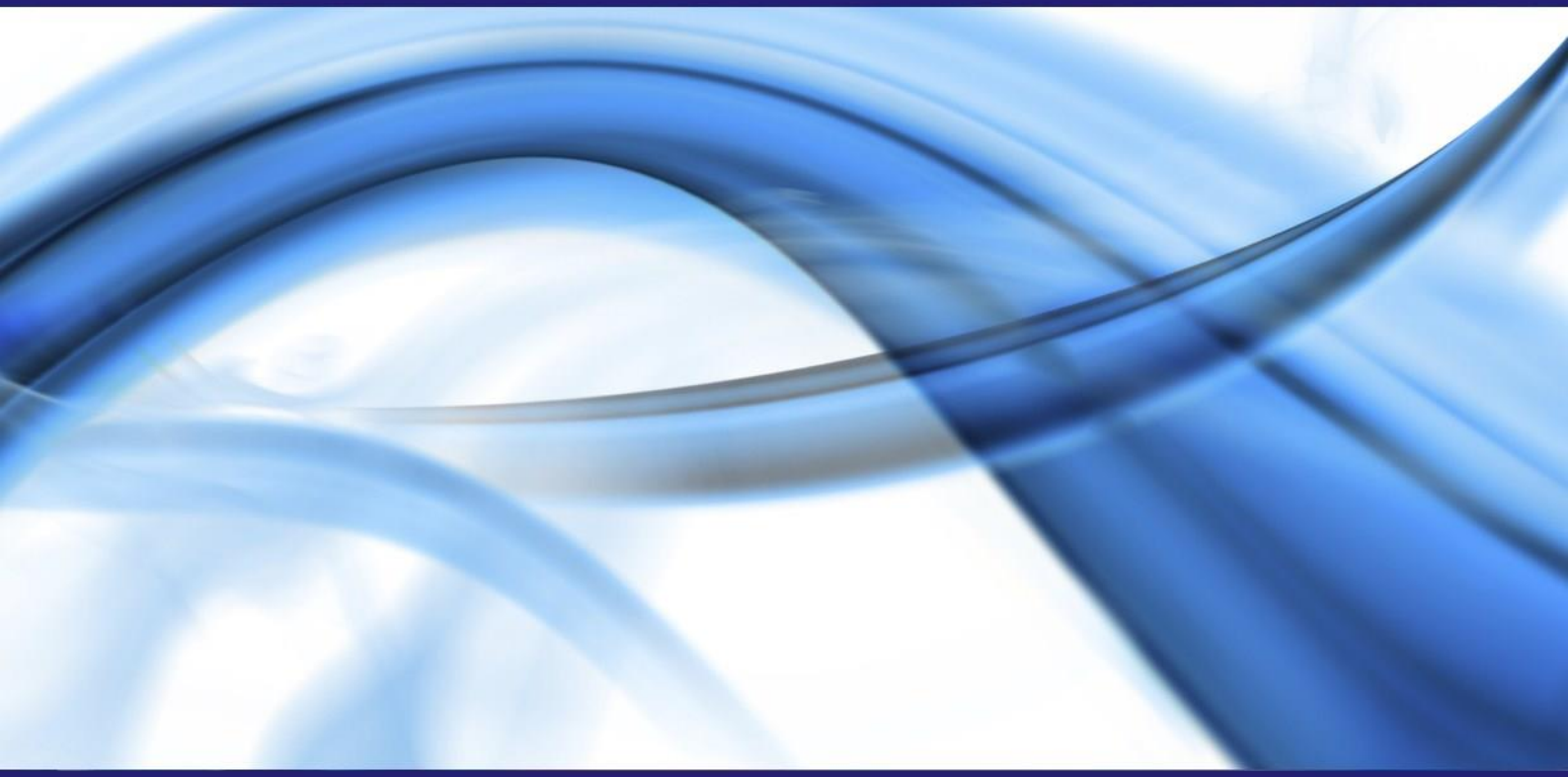
analysys mason



White paper for IBM

Automating multi-vendor service lifecycle management in an NFV-based network

February 2017

Caroline Chappell, Anil Rao

www.analysysmason.com

Contents

List of figures

1. Executive summary

This paper considers the impact of network function virtualisation (NFV) and software-defined networks (SDN) on service lifecycle management (SLM). It argues that these technologies are triggering changes in the way network functionality is managed, particularly in the cloud-native virtualisation phase of NFV.

It points out new challenges for SLM in a cloud-native network, including the way in which service fulfilment and assurance processes are integrated across network domains and operational silos. Integration itself is not a new requirement but the scale and dynamicity of the interactions between the fulfilment and assurance function is leading to a rethink of SLM architectures and support systems. New cloud-native SLM requirements and tools in turn are driving organisational change. Communications service providers (CSPs) have an extensive task ahead of them to re-educate and re-skill staff for new roles and to reshape their organisations so that they can manage the virtualised network effectively.

The paper discusses the design and runtime separation of SLM concerns which nevertheless must be addressed together through a software development and IT operations (DevOps) approach to achieve the high level of automation needed in a cloud-native network. The DevOps approach sweeps away the current waterfall model of service development where SLM is only considered once the service has been designed and thrown 'over the wall' to network operations. Runtime SLM must provide real-time and analytics-driven control of network and service components, such as virtualised network function (VNF) instances and the service chains they belong to. This is because each component is elastic, leading to rapid network change that needs to be managed on a different timescale from physical devices.

While the paper acknowledges that the terminology around SLM in the virtualised network is still evolving, it describes the need for new and emerging technologies to support it. These include VNF onboarding tools, a hierarchy of service and network orchestrators, dynamic inventory and service quality management and analytics platforms, coupled together within open and extensible software frameworks.

Large CSPs and open source communities are beginning to define these frameworks but they will require considerable resources to implement. We recommend that CSPs seek the advice and help of vendors in five key areas as they plan their migration to a cloud-native network. CSPs should look for a partner that can support their organisational transformation as this is key to the successful adoption of NFV. The need for software lifecycle management expertise and skills is new to network operations: a partner can provide training and tools here. CSPs can shorten the path to automation by working with a partner that has end-to-end management understanding of the network and deep analytics and machine learning capabilities. CSPs that want to implement an SLM framework for the cloud-native network will need a partner that can support multiple VNF vendors and NFV and SDN vendor technologies. Finally, we expect most CSPs will want to take advantage of the cost savings and operational efficiencies delivered by cloud-enabled managed services in future. CSPs should look for a partner with a strong track record in cloud-based service delivery.

2. CSPs are adopting SDN/NFV to transform their ability to deliver services

2.1 SDN and NFV enable CSPs to respond to new revenue opportunities

The ability to offer compelling services in a timely manner and at an attractive price has always been key to competitive success. Communications service providers (CSPs) face increasing competition from Internet companies that can offer their traditional services for free and deliver new services faster, with more features and lower costs. Software-defined networks/network function virtualisation (SDN/NFV) technologies help to redress the imbalance between CSPs and Internet players in this respect. They enable CSPs to gain the benefits of the cloud approaches, tools and software-driven capabilities that underpin the success of companies closely associated with the digital economy, such as Amazon, Facebook, Google and Netflix.

By turning the physical network into software components that are software-controllable and programmable, CSPs can transform the agility of their businesses. There are several facets to this agility, including speed of service development and deployment and the ability to respond flexibly to service demand over time. Analysys Mason believes that CSPs' agility strategies depend on a virtualised and programmable next-generation network (vNGN). CSPs need to be able to launch new services at least as quickly and inexpensively as digital economy leaders, testing out new ideas rapidly and on a small scale first, scaling up those for which there is market demand and killing ('fast failing') unprofitable services. In a virtualised and programmable network, CSPs can use software automation to instantiate network-based services in a matter of seconds or minutes and scale or terminate them on demand. Real-time, flexible service delivery is a critical capability in the digital services world.

NFV exploits cloud technologies that are key to service personalisation, a further distinguishing behaviour of a digital economy leader. Virtualisation and cloud automation approaches allow CSPs to 'mass produce' service instances, each of which can be configured for the specific needs of an individual customer. NFV helps CSPs to match customer requirements and what they are prepared to pay for in a highly granular way, boosting levels of customer satisfaction and stickiness.

CSPs can leverage the efficiency and flexibility of cloud-based resource utilisation and SDN's centralised traffic management capabilities to optimise service delivery, reducing network costs while maintaining and improving customer experience. Together, NFV and SDN support the rapid and automated modification of services, in response to numerous scenarios, from fulfilling new customer requests to preserving service-level agreements (SLAs), from lowering delivery costs to the integration of new features.

As a result, Analysys Mason is seeing growing numbers of commercial SDN and NFV deployments. Both technologies are the basis for a renewed CSP push into the enterprise market, for example, in search of revenue growth. Leading operators are adopting SD-WAN solutions which enable enterprise customers to select the best-performing or most cost-effective access network for any given application at any given point in time. CSPs are typically coupling SD-WAN's SDN capabilities with virtual customer premises equipment (vCPE) solutions. This enables CSPs to upsell NFV-based value-added services to existing customers and to tap new small and medium business markets which the physical network made it uneconomic for them to address.

CSPs are looking beyond the near-term enterprise revenues they can generate from software-controlled networks to the next wave of services that 5G will start to facilitate within the next three to four years. These include network slices, connected cars, robotic surgery and augmented/virtual reality. Such services will be impossible to deliver unless they are underpinned by SDN/NFV. 5G services that require network functions to

be instantiated in microseconds will depend on cloud-native virtualisation and extreme automation technologies. Their very low latency requirements will mandate the deployment of hundreds, if not thousands of VNF instances at the network edge. Similarly, CSPs will need to run Internet of Things (IoT)-based 5G on virtualised and automated network infrastructure to lower costs. Analysys Mason's IoT research shows that revenue per connection for LPWA networks will be very small – perhaps USD1–3 per device per year, yielding revenues of USD5 billion compared to USD23 billion for cellular M2M in 2025. Whatever access network is selected, to make IoT profitable, CSPs will need to build low-cost and scalable virtualised network slices rather than networks based on conventional, physical devices dimensioned for peak traffic and typically 50–60% under-utilised.

2.2 NFV and SDN change the nature of SLM

Network operations and management processes are closely tied to the technologies the network uses. SDN and NFV involve technology change as network functions and control planes are disaggregated from proprietary hardware and become independent, programmable pieces of software. This triggers changes in the way network functionality is managed and presents a new requirement to operate the novel – for network engineers – virtualised environment in which they operate.

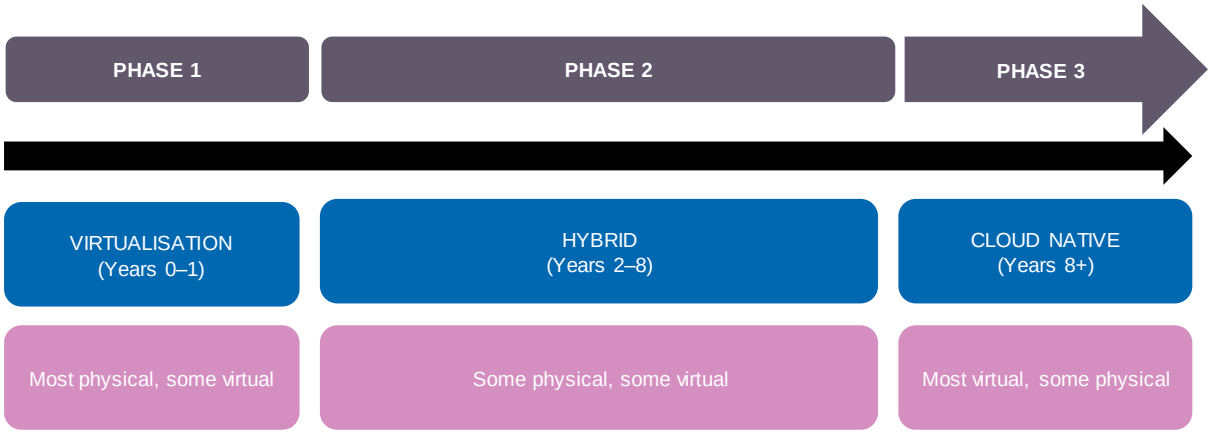
Analysys Mason identifies three phases of NFV:

- **Virtualisation**, where network function is forklifted out of its associated proprietary hardware onto COTS hardware as a first step, and subsequently placed in a virtual machine (VM) on hypervisor-enabled hardware. Both steps create a 'virtual box' that delivers some capex benefit but which, from a management perspective, is little different from the original hardware appliance. CSPs need to manage the virtualisation environment – the hypervisor and dedicated COTS hardware running the 'vbox'. But in all other respects, the resulting VNF can be managed with existing operational systems and processes.
- **Hybrid orchestration**, where multiple 'vboxes' (first-generation VNFs) run in a shared execution platform under the control of an orchestration stack. Orchestration automates the cloud management aspects of the vboxes' lifecycle (VNF instantiation, placement, scale in/out, upgrades, migration (for example, for 'recover first' remediation), termination). The new orchestration stack, known as NFV MANO (Management and Orchestration), and SDN capabilities that manage data centre/WAN connectivity between VNFs, introduce new operational processes and automation. Such vboxes still have element management systems (EMS) that are managed by traditional operation support systems (OSS) for service fulfilment and assurance purposes. VNFs may also participate in services that span the physical, as well as the virtual network. CSPs need further orchestration to manage VNFs alongside traditional physical appliances: in other words, to orchestrate across the 'hybrid' virtual/physical network. The lifecycle automation built into the MANO starts to push the need for a higher degree of service lifecycle automation/orchestration into traditional OSS, forcing change at multiple levels of the organisation.
- **Cloud-native computing,** the end goal for the ETSI[1] NFV founders who see cloud-native approaches as key to their ability to compete in the digital economy. In this phase, VNFs will be rearchitected as cloud-native applications, potentially executing alongside cloud-native IT applications in a secure, converged cloud and managed/orchestrated in a similar way. Customer-facing services will be delivered across a largely virtualised network and connectivity will be completely automated using SDN. Analysys Mason research suggests that the cloud-native phase of NFV will deliver the full benefits originally envisaged for the virtualised network: the highest levels of service agility, the lowest cost of operations, the ability dynamically to optimise service delivery based on business policies and the ability to bring new services and service features to market in extremely short timescales. But it will also be most disruptive in terms of change. Traditional manual SLM processes and OSS

[1] The European Telecommunication Standards Institute.

built for the physical network and its multiplicity of vendor-specific boxes at different network layers will need to be replaced by automated, software-driven management that is standardised across vendor VNFs, regardless of network domain.

Figure 1: Network virtualisation will take place in three phases, with different SLM implications in each phase (Source: Analysys Mason, 2017)



2.3 New challenges for SLM in a virtualised network

CSPs are aware of the benefits of implementing SDN/NFV but find their associated SLM impacts disruptive and challenging. Leading CSPs are vocal about the urgency of their need for cloud-native operations but recognise that their adoption represents the largest disruption of all. To manage services effectively in an NFV-based network, CSPs need to overcome three large challenges.

Integrating operational process management silos

In a virtualised network, the fulfilment and assurance of services is tightly coupled. A CSP's goal is to deliver to customers the right services, maintained at the right quality of service, while customers need them. During each service's lifecycle, customers may want to change service features and the quality of service they are receiving multiple times. In addition, events may conspire to affect service quality, requiring the CSP to make service adjustments. In an NFV/SDN-based network, changes triggered by repairs, upgrades, scaling events and new customer requirements will take place in close to real time. The greater the volume of changes, the more adjustments will be needed to keep service quality stable. CSPs will use the new NFV orchestration stack and SDN controllers to configure and re-configure, scale and migrate VNFs in response both to customer demand and environmental events. This will require a tight feedback loop between service fulfilment – responsible for the dynamic and continuous provisioning and re-provisioning of the service – and service assurance, which dynamically monitors service-impacting events and detects faults. Service fulfilment and service assurance are siloed lifecycle management processes in the physical network that need to be fully integrated once CSPs reach the hybrid phase of NFV.

Adopting software lifecycle automation

In cloud-native networks, VNFs are the raw resources for delivering customer-facing services. VNFs are software components and their software has a lifecycle that needs to be managed in addition to any customer-facing service ('service chain') that uses them. In fact, it is the automated ease with which network functions-as-software can be provisioned, patched and upgraded that underpins the agility and cost benefits inherent to NFV. However, the continuous integration of new VNF versions must be managed with care to avoid destabilising existing service chains. This requires the implementation of a new software development and IT operations (DevOps) relationship between VNF vendors and CSPs and new processes and tooling to support the

certification, testing, onboarding and subsequent live provisioning of VNFs. VNF vendors need to understand the operational environment that their components are required to fit into and CSPs need to have systems in place to deal with frequent software changes to VNFs during their lifetime in the network. These requirements are completely new to traditional network operations.

Addressing organisational change

The largest challenge to NFV/SDN progress is people- and culture-related. Network operations departments that have operated the network in the same way for decades are typically highly conservative, have built up a body of largely unformalised knowledge based on manual procedures, are pragmatic rather than strategic and are deeply averse to change. CSPs can find it extremely difficult to impose new SLM practices that require the development of programming skills, closer links with the IT organisation, DevOps styles of working and co-operation across network domains, all of which threaten current ways of working. Employees may have little incentive to codify their knowledge as part of a process automation exercise if they fear for their jobs. CSPs have an extensive task ahead of them to re-educate and re-skill staff for new roles and to reshape their organisations so that they can manage the virtualised network effectively.

3. SLM becomes more dynamic and automated in cloud-native networks, supported by a new operational framework approach

3.1 Network and SLM processes need to be rethought for the NFV-enabled network

Future-looking, open source-based SLM architectures distinguish between ‘design-time’ and ‘runtime’ operations. This is a useful and DevOps-oriented way of looking at the separate, but related, sets of processes associated with **designing** customer-facing services, including, simultaneously, their management aspects, and **delivering** such services. Runtime service delivery involves executing and managing the software resources from which the services are constituted, guided by the management attributes defined during service design. This is very different from current waterfall models of service development where service management is considered at a much later stage, once the service has been designed and thrown ‘over the wall’ to network operations.

Another distinction can be made between offline service management, during which services are created, and online service control which looks after these services when they are live. Online service control implies a more real-time lifecycle management environment than exists in the physical network. Such real-time and analytics-driven control is needed because the VNFs that support services are elastic, leading to rapid network change that needs to be managed on a different timescale from physical devices.

The terminology for operations in the virtualised network is still evolving but clear indications of what the new operational model will look like are beginning to emerge.

Design-time operations define services with an emphasis on composability and management-readiness

In a virtualised network, standardisation is key to achieving high levels of automation. Services need to be defined in a standardised way, together with operational parameters, such as their configuration options, KPIs and the technical and business policies that will govern their deployment across NFV infrastructure. Service

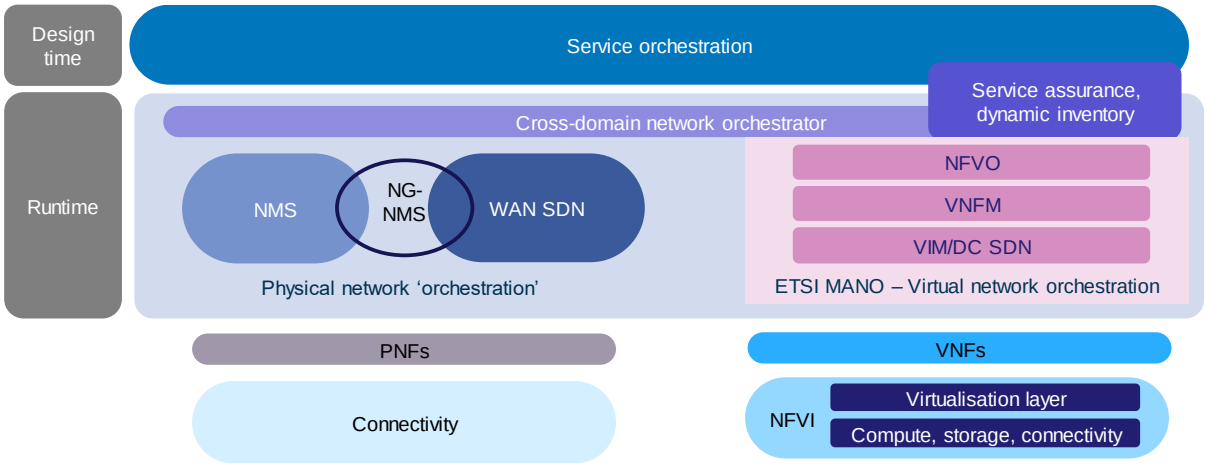
designers need one place in which to define end-to-end services at a high level of abstraction, where they don't need to worry about the exact type of vendor device(s) that will be used to support the service. Cloud-native operations will be model-driven, so all services will be described in a standardised modelling language, making it easy to reuse existing service components. Service designers can quickly compose these to create services in hours and days rather than in weeks and months.

An important aspect of design-time service modelling is that it encompasses both VNFs and service chains. This mandates a platform approach where all the capabilities that contribute to paid-for services are modelled at a similar level of granularity, as service components. Service components may be combined into larger sets, such as service chains, before exposure in the design-time catalogue. At design time, customer-facing services (paid-for products) can be composed from any combination of platform components.

VNFs are onboarded into the design-time platform and modelled as components so that they can be composed together with other resources to create new, paid-for services. In this scenario, it's important that a CSP's chosen VNF suppliers, or a VNF-neutral third party, such as a systems integrator, model the components and build the lifecycle automation scripts they need in the standard language(s) and templates used by the CSP. This ensures that VNFs' operational aspects are aligned with the CSP's runtime requirements in a DevOps manner. Because VNF vendors are at very different stages in modelling their products, CSPs are finding systems integrators helpful in building common management across VNFs and certifying their correct execution on the CSP's virtualised infrastructure.

Over time, as modelling approaches become standardised, VNFs as services may become available through the equivalent of 'app stores' from which CSPs will be able to download and manipulate VNFs at design time on demand. Eventually entire paid-for services may be templated, enabling customers to bring them to CSPs for instantiation on demand.

Figure 2: Service/network orchestration hierarchy for the hybrid network (Source: Analysys Mason, 2017)



Service orchestration bridges design and runtime environments to fulfil services

In Analysys Mason's taxonomy, service orchestration (see Figure 2) is a key process that takes a customer order, composed from the set of parameterised design-time components that specifically match the customer's needs, and co-ordinates its automated, end-to-end fulfilment across appropriate network domains. Service orchestration identifies the network domains that will be used to deliver the service based on the policies governing the service (for example, security, performance, cost) and the profiles and real-time status of each domain (for example, geolocation, high-/low-end VNF and NFV infrastructure vendors used, resource

availability). Service orchestration maintains the end-to-end definition of the service and is the starting point for SLM automation.

Service orchestration allocates component(s) to the appropriate domain, or network-level orchestrators for activation. A network orchestrator like the NFV MANO applies customer-specific configurations to existing VNF instances or creates new instances with the correct configuration, using the automation pre-defined and associated with each service component at design time. SDN controllers are a type of network orchestrator that uses automation to set up VNF connectivity. The service orchestrator verifies that all components are operational and the service is instantiated before passing runtime SLM responsibility to the network orchestration layer. The orchestrators are then responsible for managing 'their' service components/chains of components in an automated way at runtime.

Runtime operations manage services in real time, controlling cloud resources and connectivity to maintain SLAs

Runtime operations comprise the analytics-driven, automated processes that manage the lifecycle of service components both individually and in the context of their service chains. The set of domain-specific network orchestrators in a CSP's environment is key to the execution of these processes. Where service chains span multiple network domains, a **cross-domain network orchestration** (CD-NO) capability is needed in addition to individual domain orchestrators. The CD-NO talks to and co-ordinates all domain-specific orchestrators, including the NFV MANO, WAN SDN controllers and legacy network management systems, to resolve any SLM issues that may arise between them. The CD-NO benefits from a dynamic inventory that provides a real-time view of service/resource mapping. This is a federation of the real-time component management views maintained individually by each domain orchestrator.

The CD-NO and domain orchestrators also share access to federated systems that monitor and analyse end-to-end services, service components and resources in the virtualised environment, predicting degradations and detecting events that threaten service performance and SLAs. These trigger automated orchestration actions based on pre-defined management scripts, for example, actions to migrate or scale an individual VNF, adjusting connectivity through an SDN controller, or which migrate and/or reconnect an entire service chain, depending on the cause and scope of the threat. In the dynamic, virtualised network, CSPs will use anomaly detection to predict faults and use network orchestrators to move services/service components proactively. If an unanticipated fault does occur, they can re-instantiate affected components first (the 'recover first' philosophy) and look for root cause afterwards. Big data architectures and replay tools will facilitate root-cause analysis. The automated feedback loop between assurance analytics and orchestration will support continuous optimisation of the virtualised network to prevent unplanned outages.

In a cloud-native phase of virtualisation, the hierarchy of orchestrators will need to co-operate over the continuous integration of software updates and patches to the resources under their control: cloud/NFVI resources, VNFs, management components. Continuous integration may have customer-facing service impacts which the network orchestration layer will need to mitigate and manage. Automation is key since the network orchestration layer will need to respond to a continuous and real-time stream of demands, from customers making service changes, from resource suppliers to carry out updates and from services and components to help them maintain SLAs.

3.2 A new service management framework is needed to replace the assortment of siloed OSS that manage networks today

Traditional OSS are not architected to support cloud-native operations. Fulfilment and assurance systems are siloed, each supporting their own sets of processes. They are typically not designed to provide real-time, fully

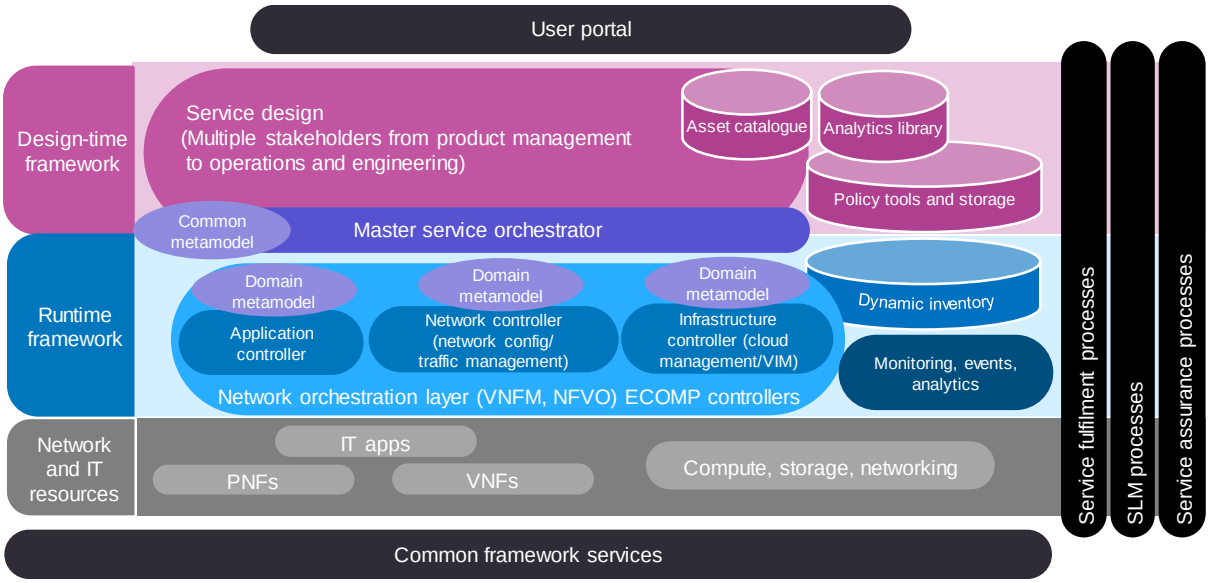
automated SLM, with closed loop feedback between processes. Inventory systems are offline and have limited ability to track dynamically changing cloud resources. Existing inventory systems have not historically had to provide the functionality in the NFV orchestration stack and SDN controllers, so they must be integrated with these new capabilities, potentially creating new silos. Extending and evolving existing systems is expensive and doesn't address key issues, such as their monolithic architectures and limited focus on managing specific types of service, network and/or vendor domain.

Leading CSPs indicate that they want future cloud-native network and service management functionality to sit within a common software framework. A software framework (see Figure 3 below) is an open and modular environment with a base set of functionality (such as role-based access controls, message handling, application programming interface (API) management, big data and real-time streaming analytics capabilities) that can be used by any other functions integrated into the framework. A software framework for cloud-native operations will contain common design and runtime management functions, including design-time tools for defining services and their associated management automation artefacts (APIs, policy/rule sets, scripts, templates, recipes, service/VNF models and descriptors), and runtime functions, such as network orchestrators, dynamic inventory, monitoring and analytics systems.

Framework providers, users and third-party partners can use open APIs to add new management functions, enriching and changing the framework's management capabilities. Some of these new functions may be sourced from open source communities. Extensibility and multi-vendor support are key benefits of a software framework approach. The framework itself will be built using cloud-native technologies and will run in the cloud, consuming cloud resources for scalability and agility. Contributors of management functions will build them as 'microservices' that lend themselves to cloud-native execution, alongside the microservices-based VNFs and service chains they will manage.

Several organisations and operators are specifying open source software frameworks to support cloud-native operations. Such frameworks dispense with OSS terminology such as service 'fulfilment' and 'assurance'. Instead, their model-driven orchestration mechanisms dynamically co-ordinate multiple management functions within the framework, including data collection, analytics and events components, the dynamic inventory and policy tools, to create and execute appropriate provisioning and assurance processes.

Figure 3: Software frameworks take a new approach to SLM across the hybrid network (Source: Analysys Mason and Open ECOMP, 2017)



4. Selecting a partner to help implement SLM in a cloud-native network

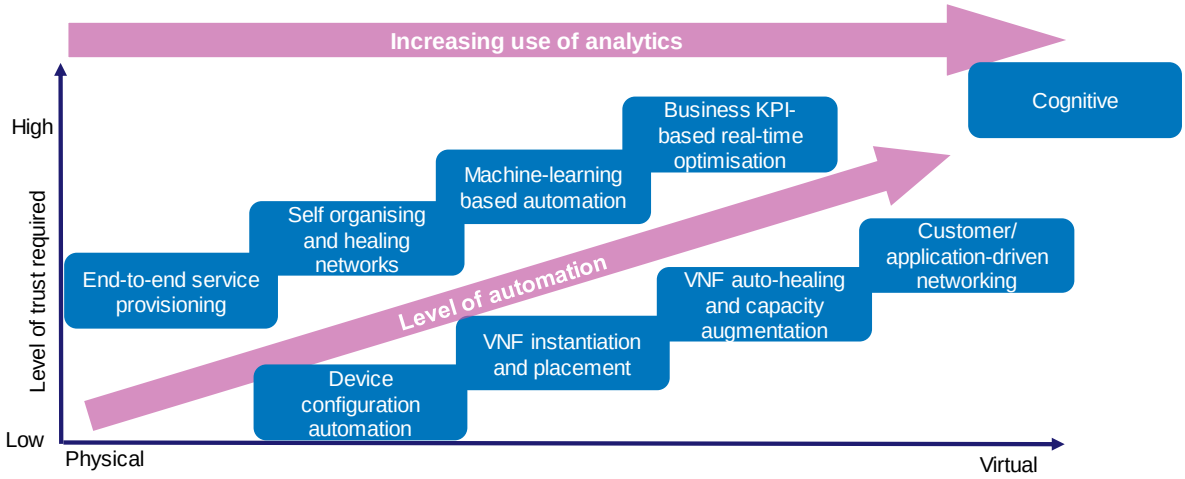
NFV and SDN are pushing extensive change into CSP organisations on multiple fronts. The amount of change can be overwhelming and most CSPs will lack the full set of knowledge, experience and skills needed for implementation success. The ability to operate an SDN/NFV-enabled network is critical and CSPs are particularly concerned with understanding and managing process and system changes associated with cloud-native operations. There are five key ways in which vendors can supplement CSPs' internal capabilities as they move towards provisioning and managing services across a cloud-native network:

1. **Support organisational transformation**: employees will not simply adopt new processes and tools because they are there. They need to be encouraged and trained to operate the network and manage service lifecycles in a different way. Organisational transformation is much harder than technology transformation but it is critical to the latter's success. CSPs can benefit from the change management experience, skills and best practices that external vendors bring to the table, which will accelerate and smooth the path of organisational change.

2. **Provide software lifecycle management expertise and skills**: SDN and NFV exploit the flexibility, programmability and agility of software: they represent a software-based revolution in the network. CSPs need to adopt software management approaches and skills, such as DevOps, agile ways of working and continuous delivery capabilities, if they are to realise the benefits of these technologies. Service delivery in the cloud-native network is a software lifecycle management challenge at multiple different levels: customer-facing services, VNFs, virtualisation layer, operational functions. CSPs historically do not have the critical mass of software skills needed to manage the cloud-native software environment, nor do they have a DevOps approach to the software lifecycle. Vendors can provide guidance and capacity.

3. **Deliver appropriate automation using advanced technologies**: automation is key to managing the dynamic and elastic nature of the cloud-native network. Automation needs to span network domains and vendors, and requires extensive integration knowledge, experience and discipline. Automation should be informed by analytics that distil the best of human knowledge and will increasingly use machine learning technologies to optimise complex service delivery requirements in the highly dynamic, software-defined environment the network will become. Such automation is not easy to build and will require an incremental approach to build operational trust (see Figure 4 below) but it is key to CSPs' ability to compete against digital economy leaders. CSPs can gain valuable insights and support from vendors with digital economy credentials, end-to-end management understanding of the network and deep analytics and machine learning capabilities.

Figure 4: Incremental automation to strengthen trust (Source: Analysys Mason, 2017)



4. **Build/contribute functions to a service management framework**: large CSPs have the resources to build their own service management frameworks. Many CSPs would prefer to acquire a framework that conforms to industry standards and is open so that they can plug in best-of-breed management functions from any vendor they choose. CSPs that want to implement a framework for the cloud-native network will look for vendors with management knowledge that spans network domains and which can support multiple VNF vendors and SDN and NFV vendor technologies. CSPs that prefer not to take a service management framework approach at this point can future-proof their choices of operational systems by insisting that these are modular and microservices-based, with open APIs, so they will fit into a framework in future.

5. **Provide managed services**: CSPs can increase operational efficiencies through third-party, managed delivery of the service management framework or selected processes and functions supported by it. Depending on the management functions that CSPs want to outsource and their cost constraints, they may consider a private or public cloud deployment. Choice of delivery model will be important here, as will the openness of the vendor's cloud solution to a CSP's other technology partners so that all the components of the CSP's SLM solution can be co-located for security and efficiency purposes.

5. Conclusion

CSPs are pressing ahead with the implementation of NFV and SDN. Leading CSPs are pushing for cloud-native VNFs and technologies as the foundation for 5G network and service innovation. Cloud-native NFV will have a disruptive impact on SLM. It requires tight, end-to-end integration between fulfilment and assurance processes through the medium of an orchestration hierarchy, dynamic inventory and service quality management (SQM) and analytics platforms, a high degree of automation to handle the real-time and elastic nature of change within a cloud-native network and organisational change as network operations adopt IT DevOps approaches and tools.

The industry has acknowledged for some time now that traditional OSS do not have the capabilities to support SLM in a cloud-native context. They will need to be superseded by an open and modular software framework approach that can accommodate SLM tools, including service, CD-NO and network orchestrators and analytics capabilities from multiple vendors. The framework should be built and run as a cloud-native system with the same properties of extensibility, scalability and resilience that are driving CSPs to implement cloud-native networks.

CSPs have significant work ahead of them to implement the new aspects of SLM that cloud-native NFV mandates. Many do not have the resources to build or migrate to a new operational framework without help. They need assistance to move to a DevOps model, where the operational automation used at runtime is developed at service design time, and services themselves are modelled and composed from standardised components. They face myriad decisions around the tools and technologies needed to build operational automation, onboard VNFs and manage the cloud-native network appropriately. Organisational change is a large challenge where CSPs can benefit from adopting tried and tested change management best practices.

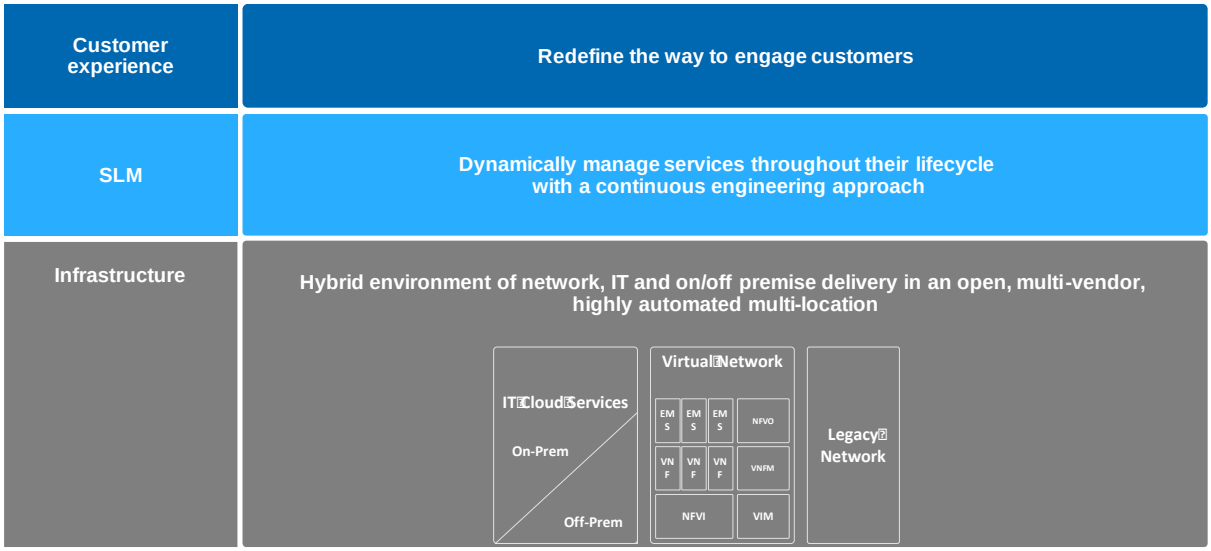
It is important that CSPs choose the right partner to support them as they establish the ability to manage service lifecycles across NFV-enabled networks. Partners with the appropriate sets of skills can considerably shorten and de-risk this journey. CSPs can achieve the full benefits of the cloud-native phase of NFV ahead of competitors, including the ability to match the service agility and operational cost advantages of Webscale players.

6. IBM – enabling automated multi-vendor SLM in cloud based networking environments

IBM identifies three layers of innovation in the cloud-based network:

1. Customer engagement: redefining customer interaction, improving the experience
2. Dynamic SLM: dynamically managing services via a continuous approach
3. Hybrid infrastructure: automating and managing virtual and physical networks, IT and networks, and a mix of on-premise and cloud-based networks.

Figure 5: The three layers of cloud-based networking (Source: IBM)



The SLM layer (see Figure 5 above) is key for service providers to be more agile in delivering innovation to their customers. IBM is focused on ways to operationalise and automate the SLM layer, building in agility using DevOps practices for design and development, leveraging cognitive service operations to maintain rich models of dynamic service and infrastructure deployment, and controlling the lifecycle with closed loop, policy-driven automation to drive service deployment and optimisation within a dynamic, hybrid infrastructure.

6.1 SLM

The goal of SLM is to shorten the time from imagining a network service to delivering it ready for customer use. Every aspect of the lifecycle designs, develops, deploys and optimises the network service continuously in an automated way on top of a dynamically changing infrastructure. Agile DevOps practices accelerate iterative service design and development. Closed loop automation speeds policy-driven service deployment and optimisation. Cognitive service operations and dynamic infrastructure monitoring provide the insight for continuous service optimisation within an infrastructure that is dynamically changing in response to usage patterns.

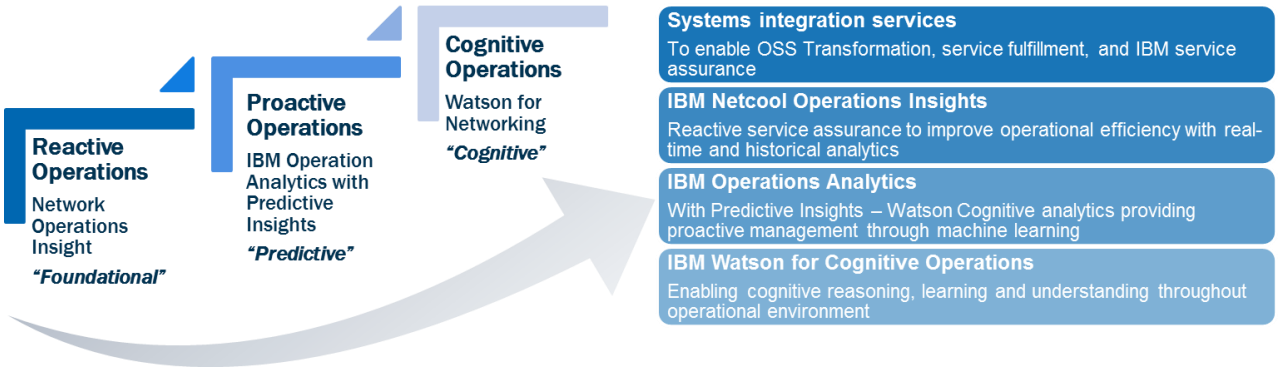
6.2 Cognitive service operations

Cognitive (predictive) analytics can detect problems as they emerge, before customers are impacted. Cognitive computing for networks can rapidly unearth problems within a fast-changing network using inherent capabilities such as self-learning and reasoning to analyse network issues. Cognitive service operations bring together

analytics and automation to reduce operations involvement and augment the capabilities of the service operations team. Cost savings are realised as services are built, deployed and operated. Analytics and automation are extended into areas of testing, closed-loop orchestration, and network operations. As analytics and automation come together, they boost speed, agility and innovation.

IBM uses Netcool Operations Insight and IBM Operations Analytics to enable real-time service operations. By augmenting these capabilities with IBM Watson for Cognitive Operations and its full range of cognitive computing functions, CSPs can transform service operations into 'cognitive' service operations (see Figure 6 below).

Figure 6: Using analytics to enable foresight and augment cognitive operations (Source: IBM)



6.3 Closed loop automation

The key to achieving a cognitive service operations based CSP is through performance analytics driven continuous closed loop orchestration, based on policy defined at initial deployment. Successful automation solutions for dynamic virtual infrastructure must understand the current service and infrastructure state, the desired service state, and the difference between them. With IBM's Urbancode Deploy and new Netcool Agile Service Management solutions, service providers can track real-time network topology and deployed components, and provide the information required for best-fit automation in a dynamic environment.

6.4 DevOps

The convergence of the 'dev' and 'ops' sides is expected to accelerate in future. The emerging area of agile network DevOps aims to combine the develop and design side of OSS with the deploy and run side. By using agile principles to develop, test, run and optimise software, CSPs can bring the power of cloud to the network. Fuelling this trend is the need to move with agility at scale, the need to harness the power of cloud technology and the need to extend DevOps tools and processes to the network. This iterative and automated approach brings together elements of operations with design, security, performance and functional verification to ensure they all are available and working together to deliver the best customer service and experience.

6.5 Conclusion

Cloud-based networking brings together the layers of the network infrastructure, the customer and the service lifecycle. CSPs can proceed with cloud-based networking while relying on the interdependencies between SLM, cognitive service operations and agile network DevOps.

IBM has helped over 4000 clients in open cloud solution delivery, and has developed deep expertise in designing, building and operating private, public and hybrid cloud environments. With one of the largest professional services organisation in IT and telecoms, IBM is well positioned as a strategic partner for CSPs that are embarking on the journey towards cloud based networking and automated SLM.

About the authors

Caroline Chappell (Principal Analyst) is the lead analyst for Analysys Mason's Software-Controlled Networking research programme. Her research focuses on service provider adoption of cloud and the application of cloud technologies to fixed and mobile networks. She is a leading exponent of SDN and NFV and the potential that these technologies have to enhance business agility and enable new revenue opportunities for service providers. Caroline investigates key cloud and network virtualisation challenges, and helps telecoms customers to devise strategies that mitigate the disruptive effects of cloud and support a smooth transition to the era of software-controlled networks. Caroline has over 25 years' experience as a telecoms analyst and consultant.

Anil Rao (Senior Analyst) is the lead analyst for Analysys Mason's Service Assurance research programme. He produces market share, forecast and research collateral for the programme and focuses on industry topics including NFV/SDN and their impact on service assurance, and the importance of service assurance in reducing churn and improving customer experience. He has also published research on IP probes, real-time network analytics and unified service assurance. He holds a BEng in Computer Science from the University of Mysore and an MBA from Lancaster University Management School, UK.

This white paper was commissioned by IBM. Analysys Mason does not endorse any of the vendor's products or services.

Published by Analysys Mason Limited • Bush House • North West Wing • Aldwych • London • WC2B 4PJ • UK
Tel: +44 (0)20 7395 9000 • Email: research@analysysmason.com • www.analysysmason.com/research

Registered in England No. 5177472

About Analysys Mason

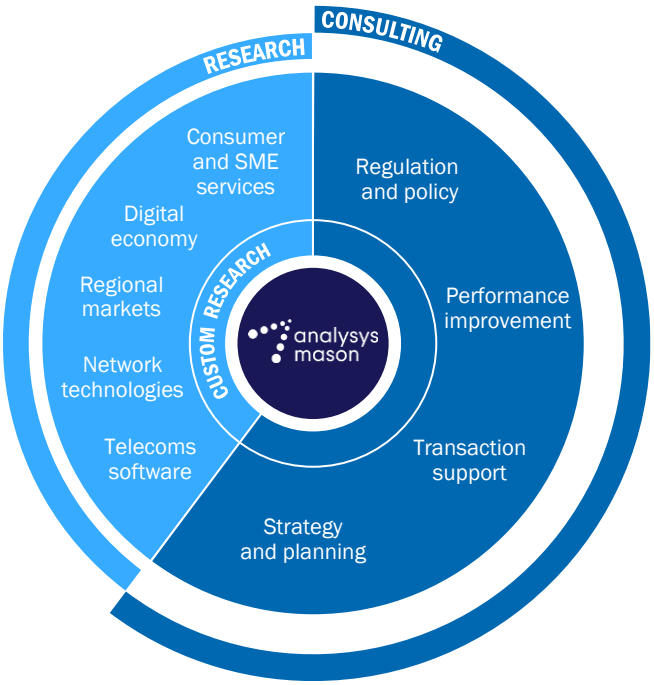
Analysys Mason is a trusted adviser on telecoms, media and technology (TMT). We work with our clients, including CSPs, regulators and end users, to:

- design winning strategies that deliver measurable results
- make informed decisions based on market intelligence and analytical rigour
- develop innovative propositions to gain competitive advantage.

We have around 208 staff in 12 offices and are respected worldwide for exceptional quality of work, independence and flexibility in responding to client needs. For more than 30 years, we have been helping clients in more than 100 countries to maximise their opportunities.

Consulting

- Our focus is exclusively on TMT.
- We support multi-billion dollar investments, advise clients on regulatory matters, provide spectrum valuation and auction support, and advise on operational performance, business planning and strategy.
- We have developed rigorous methodologies that deliver tangible results for clients around the world.



For more information, please visit www.analysysmason.com/consulting.

Research

- We analyse, track and forecast the different services accessed by consumers and enterprises, as well as the software, infrastructure and technology delivering those services.
- Research clients benefit from regular and timely intelligence in addition to direct access to our team of expert analysts.
- Our dedicated Custom Research team undertakes specialised and bespoke projects for clients.

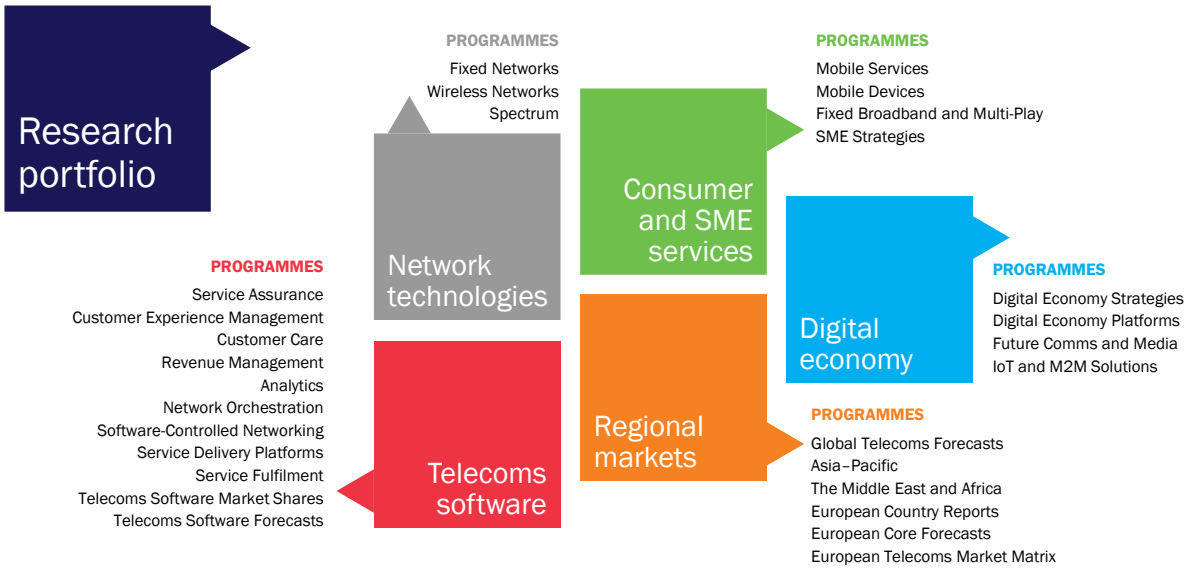
For more information, please visit www.analysysmason.com/research.

Research from Analysys Mason

We provide dedicated coverage of developments in the telecoms, media and technology (TMT) sectors, through a range of research programmes that focus on different services and regions of the world

The division consists of a specialised team of analysts, who provide dedicated coverage of TMT issues and trends. Our experts understand not only the complexities of the TMT sectors, but the unique challenges of companies, regulators and other stakeholders operating in such a dynamic industry.

Our subscription research programmes cover six key areas.



Each subscription programme provides a combination of quantitative deliverables, including access to more than 3 million consumer and industry data points, as well as research articles and reports on emerging trends drawn from our library of research and consulting work.

Our custom research service offers in-depth, tailored analysis that addresses specific issues to meet your exact requirements

Alongside our standardised suite of research programmes, Analysys Mason also has a Custom Research team that undertakes specialised, bespoke research projects for clients. The dedicated team offers tailored investigations and answers complex questions on markets, competitors and services with customised industry intelligence and insights.

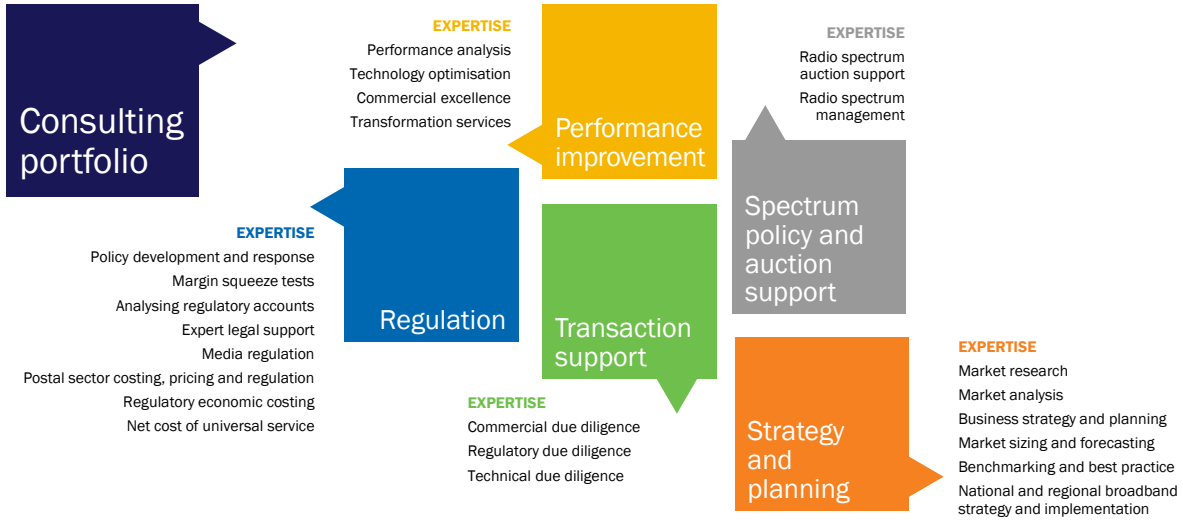
For more information about our research services, please visit www.analysysmason.com/research.

Consulting from Analysys Mason

For 30 years, our consultants have been bringing the benefits of applied intelligence to enable clients around the world to make the most of their opportunities

Our clients in the telecoms, media and technology (TMT) sectors operate in dynamic markets where change is constant. We help shape their understanding of the future so they can thrive in these demanding conditions. To do that, we have developed rigorous methodologies that deliver real results for clients around the world.

Our focus is exclusively on TMT. We advise clients on regulatory matters, help shape spectrum policy and develop spectrum strategy, support multi-billion dollar investments, advise on operational performance and develop new business strategies. Such projects result in a depth of knowledge and a range of expertise that sets us apart.



We look beyond the obvious to understand a situation from a client's perspective. Most importantly, we never forget that the point of consultancy is to provide appropriate and practical solutions. We help clients solve their most pressing problems, enabling them to go farther, faster and achieve their commercial objectives.

For more information about our consulting services, please visit www.analysysmason.com/consulting.