White paper for Accanto Systems

Choosing a VNF lifecycle management solution: Key challenges and crucial considerations for CSPs

June 2017

Anil Rao

www.analysysmason.com
Contents

1. Executive summary .............................................. 2
2. VNF lifecycle management automation is vital to attain service agility and lower operational economics ................................................................. 3
   2.1 The case for automation in NFV ................................ 3
   2.2 VNF lifecycle management and automation ................ 3
3. Poor MANO standardisation has led to diverse approaches and disparate implementations of lifecycle management .................................................. 4
   3.1 ETSI has proposed a high-level MANO reference architecture but the interfaces are open to interpretation ........................................... 4
   3.2 The emergence of a plethora of non-standard commercial orchestration solutions and open source automation frameworks is exacerbating the problem ................................................................. 5
   3.3 Two architectural approaches to VNF lifecycle management have emerged ................................................................. 6
4. Applying DevOps to NFV will be a challenge without a common approach to VNF modelling and packaging .................................................. 7
   4.1 Applying DevOps to VNF development presents challenges ................................................................. 7
   4.2 Key components to enable VNF lifecycle automation ................................................................. 7
   4.3 Need for a common approach to VNF modelling ................................................................. 8
5. Choosing a VNF lifecycle management solution ................................................................. 8
   5.1 The generic VNFM has potential to be lower cost with fewer integrations, but CSPs must clearly define and enforce the interface requirements ................................................................. 8
   5.2 The ability to provide out-of-the-box automation for advanced functions can be a formidable differentiator for VNF lifecycle management solutions ................................................................. 9
   5.3 Solutions that normalise the VNF models and interfaces for seamless onboarding and automation can future proof CSPs’ investments as standards evolve ................................................................. 9
6. Conclusions .................................................. 10
7. Accanto Systems – solution overview ................................................................. 11
   About the authors .................................................. 13
   About Analysys Mason .................................................. 14

List of figures

Figure 2.1: VNF lifecycle [Source: Analysys Mason, 2017] ................................................................. 4
Figure 3.1: ETSI NFV reference architecture framework [Source: ETSI, 2013] ................................................................. 5
Figure 3.2: Dedicated VNFM approach [Source: Analysys Mason, ETSI, 2017] ................................................................. 6
Figure 3.3: Generic VNFM approach [Source: Analysys Mason, ETSI, 2017] ................................................................. 6
Figure 4.1: Tool diversity for VNF lifecycle automation [Analysys Mason, 2017] ................................................................. 8
Figure 7.1: StratOSS Lifecycle Management solution [Accanto Systems, 2017] ................................................................. 11
1. Executive summary

Automation is key to operationalising network function virtualisation (NFV) and software-defined networking (SDN) and achieving the expected benefits such as higher service agility and lower operational economics. As CSPs make the NFV journey from basic network virtualisation to dynamically orchestrating virtual network functions (VNFs) and ultimately to a cloud native network, they will need an increasing degree of operational automation. To achieve these goals, CSPs need a new approach to software development and operations, such as DevOps. In the DevOps model, the expectation is that the VNFs and network services are designed with the associated mechanisms to operate and manage them during runtime.

VNF lifecycle automation is right at the heart of this movement. As software components deployed on a cloud-based NFV infrastructure (NFVI), VNFs are expected to be instantiated, scaled, moved and auto-healed based on the evolving service demands or network faults, and patched/ upgraded as part of a software update process. To dynamically manage and direct the VNFs through these lifecycle stages, CSPs need a VNF lifecycle manager that provides built-in automation. The European Telecommunications Standards Institute (ETSI) proposed an NFV management and network orchestration (MANO) reference architecture which has been widely adopted, and which encapsulates the VNF lifecycle management capability in a VNF manager (VNFM).

However, the industry currently faces two key areas of concern that are creating barriers to accelerate lifecycle automation. First is how to overcome the issues around poor standardisation of the MANO and the associated interfaces, which have led to diverse product implementations in the commercial vendor space and competing automation frameworks in the open source arena, creating fragmentation and market confusion. Two VNFM approaches have emerged for lifecycle management – dedicated (per VNF) and generic (multi-VNF), requiring varying levels of northbound integration with an NFV orchestrator (NFVO) and southbound integration with a virtual infrastructure manager (VIM) and, consequently, offering different levels of automation. The second area of concern is how to apply the DevOps model to NFV. In this context, there are particular concerns around VNF development and onboarding, and patching/upgrading VNFs onto the production environment without destabilising the customer-facing service using those VNFs. This is a complex problem domain to automate as these lifecycle functions and the associated processes straddle both the vendor and the CSP environments, and requires a deep understanding of the VNF behaviours and failure scenarios. Exacerbating the problem is the lack of a standard approach for modelling and packaging VNFs, and the lack of tools for codifying the automation routines.

The industry may eventually coalesce around a more well-defined standard for MANO with clear component demarcations, interface definitions, and a common approach for codifying the VNFs and the associated lifecycle automation routines. In the meanwhile, CSPs that are pressing ahead with operationalising NFV need to implement a VNF lifecycle manager that allows them to navigate their way through this phase of uncertainty. The solution should offer a favourable trade-off between providing enough abstraction to mask the issues of standardisation while also offering out-of-the-box, DevOps-based automation for most lifecycle functions with the ability to quickly enhance the solution to cover the remaining cases.

CSPs should consider three broad evaluation criteria while choosing a VNF lifecycle management solution. The solution should: support a generic VNFM approach to reduce integration overheads; provide a broad array of lifecycle automation use cases including support for advanced lifecycle functions such as auto-heal, patch/upgrade, move and backup/restore; normalise the VNF models and interfaces for seamless onboarding and consequent lifecycle automation.
2. VNF lifecycle management automation is vital to attain service agility and lower operational economics

2.1 The case for automation in NFV

Many major CSPs are in different stages of their network evolution journey towards NFV/SDN. One common theme among these CSP initiatives is their quest to achieve a future network and operational state where they can rapidly deliver new services and modify existing services at a fraction of today’s cost. Ultimately, the expectation is to drastically shrink the cycle time of designing and launching new services and generating revenue, resulting in better cash flow and achieving a stronger financial state for the CSP.

To achieve this end state of higher service agility and lower operational economics, the industry is unambiguous in its support for a new operational framework. Automation is at the heart of this new operational approach. The business case for NFV weakens or even falls apart without due consideration given to automation. The term ‘automation’ is quite broad and can be applied in various contexts. But in general, CSPs expect that ‘anything that can be automated should be automated’ – i.e. all repetitive tasks with known fall-out scenarios should be automated, and more complex workflows should be automated by applying advanced analytics paradigms such as machine learning and artificial intelligence.

2.2 VNF lifecycle management and automation

VNFs are networking software applications which are expected to behave like cloud applications, i.e. software instances that can be created and modified on demand and in near real time. It is expected that each VNF will ultimately have its own lifecycle, with the ability to be dynamically altered through a plethora of functions and based on evolving service and infrastructure performance conditions – for example, service quality requirements, network performance, or an external trigger from a higher-order management system. The ability to automate these lifecycle functions is at the heart of the new operational model for NFV.

To automate the VNF lifecycle changes, an abstraction of the lifecycle functions in the form of a lifecycle manager is necessary. The lifecycle manager will present the management functions in the form of application programming interfaces (APIs) allowing programmatic control via higher-order functions such as NFVOs. The lifecycle APIs are foundational to automate the lifecycle management of the VNFs, and will ultimately pave the way for a DevOps-based model to design, deploy and operate NFV-based services.

ETSI, which has taken a lead role in progressing NFV in the industry, has proposed a set of lifecycle functions and the associated interface definitions in a series of specification documents. In summary, the proposed functions primarily focus on the ‘runtime’ stage of the VNFs, after the VNFs are deployed in the production NFV infrastructure (NFVI) as part of service chains. Other lifecycle functions such as create, onboard and update (patch/upgrade) are excluded.

CSPs should treat VNF lifecycle management in a more holistic manner and should include both the design and runtime functions to achieve DevOps-based automation (Figure 2.1). Given the complexity of an NFV-based network, and the expectations of service agility and cost expectations, manual lifecycle management is not an option. Therefore, the question is not whether the VNF lifecycle management should be automated, but to what

---

1 Refer to http://www.etsi.org/deliver/etsi_gs/NFV-IFA/001_099/008/02.01.01_60/gs_NFV-IFA008v020101p.pdf and http://www.etsi.org/deliver/etsi_gs/NFV-IFA/001_099/007/02.01.01_60/gs_NFV-IFA007v020101p.pdf
Choosing a VNF lifecycle management solution: Key challenges and crucial considerations for CSPs

extent it can be automated. To achieve high levels of automation, CSPs are considering the DevOps model of software development and operations in which the development and packaging of the VNFs, and design of the end-to-end service chains are performed with runtime operational requirements in mind. This is discussed further in Section 4.1 of this white paper.

![VNF lifecycle diagram](https://example.com/vnf_lifecycle.png)

**Figure 2.1: VNF lifecycle**

[Source: Analysys Mason, 2017]

3. Poor MANO standardisation has led to diverse approaches and disparate implementations of lifecycle management

In principle, the VNF lifecycle management capability is encapsulated in the VNF manager (VNFM) layer, but because of the poor standardisation of MANO, there is lack of clarity on the functional demarcations between the MANO layers such as NFVO and VNFM.

3.1 ETSI has proposed a high-level MANO reference architecture but the interfaces are open to interpretation

A handful of network equipment providers (NEPs) have dominated the communications networking value chain for several years. Arguably this has been advantageous to some extent, as having fewer actors to deal with may have alleviated the scale of the standardisation and interoperability problems. On the other hand, the complexity of the technology and the high R&D costs involved in producing network equipment with embedded software on proprietary hardware have created high barriers to entry. To a certain extent, the emergence of NFV/SDN democratises the network, disaggregates the value chain and lowers the barriers for new entrants (VNF developers). Most CSPs believe that, in the long term, this will create an environment for open innovation and provide a significant boost to the telecommunications industry. In the short term, however, even with a limited set of VNFs available in the market from the traditional NEPs, CSPs face issues due to lack of standards with respect to MANO and VNF lifecycle management.
Choosing a VNF lifecycle management solution: Key challenges and crucial considerations for CSPs

© Analysys Mason Limited 2017

Poor MANO standardisation has led to diverse approaches and disparate implementations of lifecycle management.

The issue of standardisation has been tackled to some extent by ETSI, who has proposed an NFV reference architecture (Figure 3.1). However, while ETSI has done a good job in laying the foundation for the NFV operational architecture, the implementation details have been left to the vendors and CSP ecosystem. This has resulted in a disparate set of products and implementations of the MANO stack.

### 3.2 The emergence of a plethora of non-standard commercial orchestration solutions and open source automation frameworks is exacerbating the problem

The industry has been flooded with numerous NFV orchestration frameworks, both in the open source arena and the commercial software vendor space. Each implementation is loosely based on ETSI’s MANO reference architecture and recommendations. However, the implementations all differ to varying degrees. This variation is primarily due to the lack of MANO standardisation (as discussed in Section 3.1 of this paper). In the open source sphere, there are at least two mainstream NFV orchestration solution frameworks: ONAP (merger of ECOMP and Open-O) and OSM. There are also numerous commercial solutions, with some employing a combination of open source components and proprietary development, and others choosing to develop entirely proprietary software. Examples include Nokia CloudBand, Ericsson DSM, Huawei Cloud Opera, HPE Network and service director, Cisco NSO, Amdocs NCSO and Netcracker AVP, among others.

The abundance of non-standard solutions has both positive and negative implications for the industry. On the positive side, more solutions in the market mean more options for the CSPs. However, there are also two primary negative implications:

- **First**, VNF vendors must cope with all the associated VNFM northbound interface specifications. These specifications tend to be dissimilar, creating additional work for the vendors. One could argue that this is not a problem as the interface definitions should adhere to ETSI specifications. The reality is that the implementations are based on the vendor interpretation of the specifications. In particular, open source solutions present a key challenge because the community focusses first on developing the code based on loose specifications, and then gradually evolving it to de-facto standards by gaining wider adoption.

- **Second**, many vendors are ‘full-stack’ NFV solution providers, i.e. VNFs, VIM (VMWare or an Openstack flavour), VNFM, NFVOs and service orchestrators. These full-stack solutions are pre-integrated and engineered to deliver the best performance when all the software layers of the stack are from a single vendor. This is not necessarily a problem – these solutions are ideal for turn-key deployments. However, the solutions may lack clear functional demarcations between modules, such as between the VNFM and the...
Choosing a VNF lifecycle management solution: Key challenges and crucial considerations for CSPs

Poor MANO standardisation has led to diverse approaches and disparate implementations of lifecycle management element manager (EM) or between the NFVO and the VNFM, and may cause integration issues and duplication of functions in multi-vendor deployments. As a case in point, the VNF lifecycle management responsibilities are shared between the EM and the VNFM, and there is lack of clarity on the boundaries between these modules. In general, the VNFM is used for the FCAPS\(^2\) of the software artefact, and the EM for the semantic aspects of the VNF functionality (e.g. signalling issues in the vEPC). This FCAPS separation was not necessary in physical networks because the software was embedded in the hardware. However, the disaggregation of the software and hardware in VNFs has made it cumbersome to separate the FCAPS functionality, resulting in coarse grained and poorly differentiated interfaces, and making it difficult for the orchestration solution vendors to create the right integrations to distinguish and extract the information they need.

Regardless of the CSP strategy to deploy NFV MANO – be it an open source framework, a commercial software strategy or a combination of both, the industry needs to standardise the VNF lifecycle management functions and the associated interfaces, and agree on the functional demarcations between the MANO layers.

3.3 Two architectural approaches to VNF lifecycle management have emerged

Based on ETSI’s proposals, multiple architectural options for designing and deploying MANO have emerged. In the specific context of VNF lifecycle management, two architectural approaches are being considered:

- using dedicated VNFM(s) supplied along with the VNFs by the VNF vendor (Figure 3.2)
- using a generic VNFM (or a set of generic VNFM(s)) with the ability to manage a set of VNFs (Figure 3.3).

\[\text{Figure 3.2: Dedicated VNFM approach [Source: Analysys Mason, ETSI, 2017]}\]

\[\text{Figure 3.3: Generic VNFM approach [Source: Analysys Mason, ETSI, 2017]}\]

There are pros and cons to these approaches but in both cases, the VNFM(s) must integrate northbound with the NFVO and southbound with the VIM. For example, in the case of the dedicated VNFM approach, CSPs must deal with a large-scale systems integration challenge as every VNFM must integrate with the NFVO and the VIM. Furthermore, the VNFM(s) may all have varying levels of lifecycle management capability which the NFVO may need to compensate for, perhaps leading to hard-coding of VNFM functionality in the NFVO. This may be undesirable given the already complex nature of the NFVO, whose primary responsibility is to manage the end-to-end network service chains of VNFs rather than managing individual VNFs.

In contrast, a generic VNFM only needs a single interface with the NFVO, while enforcing commonality of management function across multiple VNFs. In this case the burden of integration with the multiple VNFs lies with the generic VNFM but reduces the overall architectural complexity of the MANO stack. The drawback of this approach for CSPs however is that it may lead to vendor lock-in with the generic VNFM vendor.

\(\text{FCAPS = fault, configuration, accounting, performance, security.}\)
Applying DevOps to NFV will be a challenge without a common approach to VNF modelling and packaging

4.1 Applying DevOps to VNF development presents challenges

In the prevalent waterfall model of service delivery, the network functions, network services and the operational support software are designed and deployed through lengthy development cycles, and handed over to the operations department. However, the operational requirements for NFV renders this model obsolete and calls for a more collaborative approach to service delivery in the form of DevOps. CSPs intend to apply DevOps for the VNF development stages where the VNFs are created, tested and onboarded, and new patched/upgraded versions are continuously integrated into the live service chains. Subsequently, when the VNFs become part of the service chains, other lifecycle functions such as reconfigure, move, scale and heal are applied.

A webscale player which is developing its own software also controls the development of the tooling and automation. A key problem with applying DevOps to VNF development is that the VNFs are developed by third parties – DevOps doesn’t start inside the CSP. The vendors must therefore become an important part of the DevOps process. This is especially critical for the automation of VNF patches/upgrades to ensure that the continuous integration of new VNF versions doesn’t break the existing service chains.

To tackle this challenge, 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. An important aspect of this solution is to define the management aspects (e.g. operational key performance indicators) of the VNFs quite early on during the design stage and to supplement these management aspects with the rules to trigger the management routines. During the runtime operations, these management routines are automatically triggered and executed on the VNFs that constitute the service, guided by the operational attributes defined during the design stage.

4.2 Key components to enable VNF lifecycle automation

The mechanism to achieve VNF lifecycle automation is provided by two key artefacts: the VNF descriptor (VNFD) and the automation components.

1. The VNFD is created in the form of a text file and is used to describe a particular VNF’s deployment and operational instructions, and the policies and guidelines required for its lifecycle automation. For example, the VNFD includes descriptions pertaining to the infrastructure resources and configuration options to instantiate a particular VNF, instructions to auto-scale, parameters to be monitored, rules to trigger scaling function, which software components should be scaled, and so forth. Examples of VNFD modelling languages are Openstack/Heat Orchestration Template (HOT), Ubuntu Juju and OASIS TOSCA.

2. In addition to VNFD, supplementary automation components are required to, first, construct the automation routines and, second, to execute the routines in an orderly manner and deal with exceptions and fall-outs. The VNFD is ingested into this automation component which will then execute or ‘orchestrate’ the necessary workflows to automate the lifecycle functions. The guidelines on how to execute the automation scripts and workflows are also codified in the VNFD. However, there are a variety of different tools to develop these automaton components. Examples of the tools include Ansible, Puppet, Chef, Openstack Mistral, SaltStack, Python and Yang.
4.3 Need for a common approach to VNF modelling

The diversity of tools and approaches is a significant area of contention in the industry. To some extent, these diverse approaches to modelling and packaging are causing confusion and creating market fragmentation. In some cases, due to the lack of standardisation of the modelling language and tools, vendors are racing to develop solutions that are compliant with most or all the options. In other cases, vendors are declaring their allegiance to one approach and progressing their solution development.

A common approach to VNF modelling and interface definitions would go a long way in accelerating the VNF lifecycle automation initiatives in the industry and making DevOps truly effective. Consequently, vendors can develop and package the automation with high confidence knowing that the VNFs will work error-free upon onboarding into a CSP environment over which they have no DevOps control.

5. Choosing a VNF lifecycle management solution

5.1 The generic VNFM has potential to be lower cost with fewer integrations, but CSPs must clearly define and enforce the interface requirements

CSPs are considering both dedicated and generic VNFM architectural approaches and making choices based on various factors such as feature/function availability, operational readiness and skills availability. Market pressures and aggressive internal deadlines to launch NFV-based services may force CSPs to make some tactical decisions. In making these decisions, CSPs should not lose sight of the automation requirements.

Dedicated and generic VNFM approaches offer different levels of automation but it is fair to assume that in the case of dedicated VNFM approaches, the software dependencies and integration overheads are significantly higher and may increase the cost of automation, especially because of lack of interface standardisation. The generic VNFM approach has fewer integrations and may be more favourable to achieve a high degree of lifecycle automation. However, to make the generic VNFM approach a success, CSPs should take a leading role in defining and enforcing interface requirements to its vendor partners.
Choosing a VNF lifecycle management solution: Key challenges and crucial considerations for CSPs

5.2 The ability to provide out-of-the-box automation for advanced functions can be a formidable differentiator for VNF lifecycle management solutions

A VNFM must support a fundamental set of lifecycle management functions and provide the necessary automation, which should be made available for external consumption via open APIs. Many lifecycle management solutions tend to showcase the scaling function as their key strength. However, CSPs and vendors accept that more advanced functions such as heal and patch/upgrade are much harder to automate. The wide variety of potential use cases, failure scenarios and the dependencies on other VNFs and service chain elements make it extremely complex to develop automation with minimal hardcoding.

5.3 Solutions that normalise the VNF models and interfaces for seamless onboarding and automation can future proof CSPs’ investments as standards evolve

As more VNFs start to enter the market, there is a risk that they won’t all follow a modelling approach or toolsets preferred by individual CSPs. To limit the integration effort required to onboard these VNFs, CSPs should consider a lifecycle management solution that can ingest the diverse VNFs and the associated models, package them in the CSPs’ chosen model formats, and present the capabilities through open interfaces. By normalising the models and interfaces at this early stage, CSPs can expect a seamless onboarding process, and subsequently, can achieve more homogenous lifecycle operations and automation across VNFs.
6. Conclusions

The issues surrounding the standardisation of MANO, the interfaces and the tools for VNF modelling and packaging are barriers to NFV automation and operationalisation. CSPs and vendors are working with de-facto standards to circumvent the issue and are garnering broad industry support for those approaches. This has led to some positive outcomes in the way of reducing the number of viable approaches, but there is, however, a sustained level of fragmentation. There are a variety of commercial and open source implementations of the MANO, two VNF lifecycle management approaches and many tools for VNF modelling and automation. CSPs need a way of dealing with this diversity while the industry works towards standardisation.

CSPs should choose a VNF lifecycle management solution that caters to the plurality of approaches by normalising the VNF models and interfaces, providing automation for a broad set of basic and advanced lifecycle functions. CSPs should also preferably support the generic VNFM approach to reduce integration points, and should provide abstractions for both physical and virtual network functions. The VNF lifecycle management should demonstrate a level of flexibility, which will enable the system to gravitate towards the preferred standards when these eventually materialise.
Choosing a VNF lifecycle management solution: Key challenges and crucial considerations for CSPs

7. Accanto Systems – solution overview

Today’s physical network appliances require highly manual processes to manage their end to end lifecycle. Testing, installation, configuration, and problem management of network appliances all revolve around manual activities that often require a physical truck roll or a human to run each lifecycle process. NFV’s software paradigm promises fully automated lifecycle processes for bringing network services into production and maintaining them thereafter. VNFs allow a much simpler set of lifecycle tasks enabling near full automation of the creation and healing of virtual services than is possible with their physical counterparts. However, to exploit these capabilities offered by the VNFs and to achieve NFV’s promised levels of automation, a radically new lifecycle management approach is required.

Third party VNF software must be wrapped in a well-tested standard lifecycle interface to ensure no errors occur during production. Service bundles of multi-vendor VNFs must be tested for interoperability and performance; and finally, when put into production, services and VNFs must constantly be created, configured, updated, scaled, healed, and migrated with no human intervention. VNF and services on-boarding requires a comprehensive release management strategy and suite of tools and lifecycle integration framework that accommodates the variety of third party VNF software package formats. Continuous in-life orchestration also requires a new approach to modelling and managing the complexity of in-life network function lifecycle management.

*Figure 7.1: StratOSS Lifecycle Management solution [Accanto Systems, 2017]*

The StratOSS Lifecycle Manager from Accanto Systems (Figure 7.1), provides a comprehensive services design, testing and automated deployment platform addressing the challenges and complexities of the NFV paradigm. It provides a complete DevOps toolchain that manages the end-to-end lifecycle of virtual network services, from release management of VNF software packages to the continuous orchestration or running VNF and Service instances.
The solution offers three core capabilities, as follows:

A. StratOSS LM Resource Management Framework

- VNF Lifecycle Integration – standardised state model and interface for rapid on-boarding and high levels of automation.
- VNF Building Blocks – quickly wrap third party VNF software into agile service building blocks that can be tested individually for performance and to reduce errors that need manual intervention in production.

B. StratOSS LM Continuous Integration and Deployment

- Agile Service Assembly – quickly assemble versions of services from VNF building blocks while testing interoperability and healing scenarios that further reduce automation errors.
- Continuous Deployment – automatically test and certify VNFs and services across development, test and production environments.

C. StratOSS Intent Driven Operations

- Intent driven orchestration – automatically create, update and migrate services across multiple data centres based on current topology.
- Online Service Healing – automatically diagnose service issues and heal running VNFs and Services with no down time.

For further information about Accanto Systems go to: www.accantosystems.com
Choosing a VNF lifecycle management solution: Key challenges and crucial considerations for CSPs

About the authors

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 Accanto Systems. Analysys Mason does not endorse any of the vendor’s products or services.
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 215 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.