WHITE PAPER

BRIDGING THE IT/NETWORK OPERATIONS GAP TO ACCELERATE NFV DEPLOYMENT AND ACHIEVE OPERATIONAL EXCELLENCE

Dell EMC and MST Consulting provide insights and perspectives into key pitfalls and lessons learned

Authors

- Michael Sullivan-Trainor, Principal Consultant, MST Consulting, Inc., mstrainor@mstinsight.com
- Larry Rouse, Principal Consultant, Dell EMC, larry.rouse@dell.com
- Laddie Suk, Director, Digital Transformation and Industry Solutions, Dell EMC, laddie.suk@dell.com
- Joshua Zelenka, Director, Data Strategy and Governance, Dell EMC, joshua.zelenka@dell.com
- Mahesh Seshadri, Senior Director, Telecom Services, Dell EMC, mahesh.seshadri@dell.com

TABLE OF CONTENTS

LIST OF FIGURES

To learn more about how Dell EMC products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller, visit dellemc.com.

Part Number H16925

1 EXECUTIVE SUMMARY

Communication Service Providers (CSPs) are facing profound changes to their existing operating model due to the emerging competition from cloud-powered Internet players. This competition is driving CSPs to adopt a cloud-based, efficient, agile and profitable service delivery model. While transformation and adoption of technologies such as Network Function Virtualization (NFV) are critical enablers, CSPs find they are hampered by existing legacy processes that slow their transformation. Even early adopters of NFV have not reaped the expected benefits as they have faced numerous obstacles, such as repeating the silo-building approach of the past or relying too heavily on a single-vendor solution. Overall, our research finds that most IT and network organizations lack the skill set and best-fit approach to tackle the varied and complex requirements of this urgent transformation of technology, business model and operating model.

This white paper explores three recent CSP NFV implementations that experienced many challenges and delays, leading to lower than expected results. It outlines a new agile consulting approach for implementing and operationalizing a NFV CSP cloud that reduces time to market, reduces OPEX and solves organizational chaos. This new methodology will then be applied to the three case studies to show it would have mitigated the challenges experienced in each respective case study. Finally, summaries of lessons learned and new techniques for CSPs to achieve operational excellence are provided.

Combining Dell EMC's heritage of more than 2,000 successful cloud implementations with our robust NFV product and services portfolio, Dell EMC's Consulting Services organization is uniquely positioned to act as an advisor to CSP executive management. Our approach is to help navigate through the myriad choices and, together with heavy involvement by CSP management and team members at all levels, determine the most appropriate model and vendor solutions for the CSP.

2 INTRODUCTION

The 24x7 anytime, anywhere, on-demand consumer expectations are putting immense pressure on all businesses: adopt or fall behind. No industry segment feels this pressure more than today's CSPs—they have to adopt a new operating model for an excellent customer experience or lose to their competition. The current conventional delivery model founded on building out broadband capacity to gain a foothold in content and media delivery has reached its limit. In addition, the speed and efficiency to develop and deliver new services has become critical for survival in the new world. Today, when the business wants to offer a new service, the cost and time lag to deploy and operate the new layers of physical infrastructure and operational elements to support the new service exceed CSP's capacity to generate sufficient profitability. This reliance on legacy network infrastructures is leading to stagnant revenue growth and ultimately threatening the survival of the business. The key question has become *how can a CSP deliver new innovative business models and services faster and efficiently*?

To address these challenges, CSPs are embracing a new operating model that enables them to shift network capacity to where it is most needed in order to offer new services on demand at web scale, emulating the most successful cloud providers. However, most CSP organizations are ill-equipped to achieve this vision. Many lack the necessary skills to operate a multimodal environment consisting of a combination of legacy and virtual network infrastructure. Unlike transitions of the past, the new service oriented business model requires deployment of disruptive technologies such as: Management, Automation and Orchestration (MANO), NFV and Software Defined Networks (SDN) that contradict the node-based, siloed operating environments of current CSP business processes.

This white paper explores the obstacles CSPs face to achieve the new model and present an approach to quickly overcoming the challenges and with minimal expense. CSPs who take this new approach will accelerate the pace of deployment and realize a new financial model that will increase revenue, while decreasing operating costs.

3 IMPROVING RETURN ON INVESTED CAPITAL (ROIC)

Setting aside the industry metrics of average revenue per user (ARPU)—which has been falling—and operational expenditures (OPEX)—which has been rising in the current model—financial analysts typically measure CSPs by their dividends and by their returns on invested capital (ROIC). ROIC measures how much investors can expect in return for their capital. As such, it provides insight into the whole business, not just the returns on a given service type or domain investment. This measure consolidates the ultimate value of virtualization investments—namely lower OPEX, lower capital expenditure (CAPEX), as well as revenue growth.

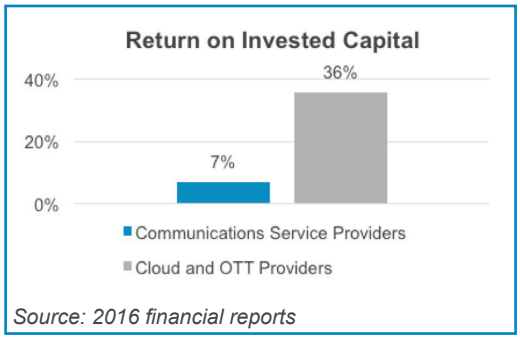
NFV, SDN and MANO technologies can make significant impact on improving ROIC by making the business of the network simultaneously less expense-intensive (both CAPEX and OPEX) and more agile in generating new revenue-producing services. The successful deployment and operation of these technologies refocuses the investment decision of CSPs away from how much money can they save in each domain, toward how much new service revenue can they add.

This refocus is a direct match for the new service areas that offer significant incremental revenue opportunities, addressing a larger customer base, plus a few single service solutions (such as the voice and data access services of the past) that generate large scale revenue. These incremental revenue opportunities include:

- The plethora of industry applications for the Internet of Things
- New use cases and services (VR, AR) made possible by the flexible bandwidth on-demand capabilities promised with 5G
- The myriad add-on services for consumer content delivery
- New services for enterprise cloud and virtualized data center infrastructure

The result is a business and financial outlook for CSPs that approaches that of FANG companies (FANG is a Wall Street term for the group performance of Facebook, Amazon, Netflix and Google). FANG financials are characterized by low margins, high sales and high returns, which are subsequently amply rewarded by obscenely high stock valuations.

For example, as shown in Figure 1, Cloud/OTT providers like Amazon boast an annualized return on capital of about 36% five times that of CSPs like AT&T at 6.7%, according to company financial reports. While there are CSPs with better and worse performance than AT&T, the company is an interesting example to follow as AT&T Labs CEO Krish Prabhu famously stated that NFV/SDN will save the company 40% to 50% in OPEX over the coming years. (Prahbu made these statements to industry and media in 2016). His qualifier on this savings prediction was that the savings will not occur until the network functions are software controlled, replacing many manual operations—in essence not until a new operational model is in place. Since AT&T is on a roadmap to virtualize 75% of its network in three years (2020) and is a leader in the creation of homegrown/industry standard MANO solutions (ECOMP/ONAP), the company deserves watching, especially from a ROIC perspective. AT&T and other early adopters have found the most success in NFV/SDN-based business services (Figure 2), but much more work needs to be done to realize the benefits in a way that positively impacts the business model.



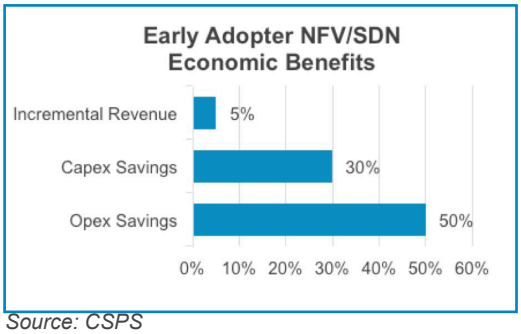
Source: 2016 financial reports

Figure 1. Provider ROIC

Cost Savings & Revenue Generating NFV/SDN Business User Services Deployed by CSPs	
Application	**Description**
Remote VPNs	Site-to-site VPN provisioning without sending skilled engineers to remote locations.
Hybrid WAN/Performance Management	Deploy multiple uplinks that both remain active during provisioning and steer application traffic based on policies such as network performance.
Virtual Network Service	Deploy virtual Firewalls to the edge to offload Internet traffic from enterprise WAN.
Dynamic Provisioning	Provide dynamic and centralized policy management in the cloud and automatically distribute the policy to the edge.
WAN Optimization	Deploy a virtual WAN optimization appliance to the edge to improve traffic throughput. Typical global enterprises use a physical WAN optimization device behind the CPE devices which requires physical wiring on customer premise. All the physical aspects are replaced by a virtual WAN appliance.
Software Defined Security	Flexible perimeter security based on distributed applications preventing DOS, credential and theft threats.
Source: CSPs	

Figure 2. CSP Business Services

4 ACHIEVING RESULTS



Source: CSPS

Figure 3. NFV/SDN Benefits

While the march to improve ROIC is a long term challenge for CSPs as they pursue FANG-like financial and operational models, AT&T and other early NFV/SDN adopters have reported immediate cost savings and increased incremental revenue results. AT&T FlexWare, an NFV/SDN service formerly known as Network on Demand, offers business customers the option to set up multiple Virtual Network Functions (VNFs) on a managed network, including bandwidth management, virtual routers, firewalls and other security applications. Benefits include deploying small or multi-country network applications through a single self-service portal, incorporating fast order processing and simplified operations. Launched in 2015, AT&T claims 1,700 business organizations are using FlexWare with availability in 150 countries, according to AT&T's business services we site in mid-2017.

As shown in Figure 3, CSP early adopters are beginning to prove the business case for NFV/SDN. Specific examples include:

- AT&T, in addition to operational cost savings from not having to deploy staff on site at customer locations, is averaging 5% incremental revenue per site from up-selling its FlexWare services. Add this revenue to the net new business AT&T is gaining from offering business services in country markets that it previously could not serve due to a lack of physical infrastructure, and the value of the implementation appears quite significant.

- China Unicom has reported a 50% OPEX reduction per value added service for its NFV/SDN deployments. The savings stem by reducing provisioning time from 60 days to just seven.

- NTT reports 50% to 80% savings in provisioning time for SDN-based VPN consolidation and has acquired SDN platform Virtela for $525 million to deliver a complete suite of SD-WAN services, including monitoring services for network performance reporting to end customers.

The above cases confirm a study by Arthur D. Little and Nokia/Alcatel-Lucent Bell Labs that highlighted operational savings of 25% to 40% for simplified fulfillment and assurance processes due to MANO and NFV. The study highlighted €39 Billion savings if European operators switched to the new NFV/SDN/MANO physical network and Operating Model.

5 DELAYED ADOPTION

With early deployments providing positive indications of economic benefits and the long term financial model driving CSPs to the goal of improved returns, it is noteworthy that the current pace of NFV/SDN/MANO adoption is relatively slow, if not stalled, due to the disruption caused by the implementation challenges with the new model.

While the market may be nearing a tipping point, where the thus-far tactical, largely cost reduction-motivated NFV business cases give way to strategic long term business cases to deploy significant digital services platforms, most of the activity remains with a small number of Tier 1 CSPs (See Figure 4). In addition, most of the CSP activity has been in pockets of the network, specifically Enterprise WAN or mobile core.

CSPs Leading NFV/SDN Deployments			
COMPANY	**LOCATION**	**COMPANY**	**LOCATION**
AT&T	North America	Orange	EMEA
British Telecom	EMEA	SK Telecom	Asia Pacific
China Telecom	Asia Pacific	Telefonica	Europe and Americas
Deutsche Telecom	EMEA	Telstra	Asia Pacific
Korea Telecom	Asia Pacific	Verizon	North America
NTT DoCoMo	Asia Pacific	Vodafone	EMEA

Figure 4. Early Adopter CSPs/SDN Benefits

6 OBSTACLES TO DEPLOYMENT

CSPs, already somewhat reluctant to disrupt their financial and Operating Models, often face additional implementation challenges. These include an immature toolset (including software that is not carrier grade), the lack of standardized orchestration and management platforms, a lack of sufficiently skilled staff and no internal education courses available to train internal staff. Moreover, integrating NFV, SDN and MANO platforms with existing networks and OSS/BSS remains a major driver of complexity, time lag and cost.

Current CSP Answers to NFV/SDN/MANO Complexity Challenges	
DEPLOYMENT OPTION	**NFV COST IMPACT**
1. Wait and See	Costly catch-up delay
2. Do it Yourself	Lost benefit of industry economies of scale
3. Build NFV Domain Silos	Mitigate ability to deploy network-wide automation
4. Rely on Single Vendor	Lose value of open source standardization and community solution development
Source: CSP interviews	

Figure 5. CSP Approaches to NFV

For many early adopters, deployments began with proof of concepts in their own or supplier labs. While the implementation of virtualized functions worked in the lab, performance and orchestration issues became evident when the solutions were deployed in CSP production environments. While the virtual functions could be implemented manually using dedicated resources in the lab, advanced resource management was lacking

to automatically balance and rebalance performance requirements across shared pools of compute and storage resources. In some instances, the VNF function would consume all the resources required as it scaled, causing co-located functions to fail. In addition to diminishing CSP staff confidence in early NFV implementations, issues such as lack of automation, performance and lack of standards made the scaling of the platforms across the multiple functions required to provide a service a highly complex proposition.

To address these issues, CSPs are taking one of four paths (See Figure 5):

1. **Wait and See**: Many Tier 2 and 3 CSPs are daunted by the complexity which they cannot afford to address, so they are adopting a wait and see attitude, hoping Tier 1s and early adopters as well as the industry will solve the problems and they can adopt later, in a cost efficient way.

2. **Do it Yourself**: A few Tier 1s are assigning dedicated staff to solve the problems internally. This approach results in CSP-specific complex architectures needing millions of lines of code to create new operational tools and platforms.

3. **NFV Silos**: Other CSPs are reverting to the build out of virtual functions in silos (with resources dedicated to each new solution). This approach replicates the domain-by-domain operational environment that network staff is accustomed to, but limits efficiency and the ability to cross-domain automate processes.

4. **Single Vendor**: Still other CSPs are turning their challenges over to a single vendor solution, replicating and reinstating the longstanding dependence on vendors to enable new business models. This approach results in vendor lock-in and the concomitant high cost and inflexibility that was the original genesis for NFV.

None of the above approaches provide the economic or agility benefits that are required to move the needle on the financial equation of CSP return on investment. Do it yourself approaches are expensive when faced with hiring new software and cloud-savvy staff, retraining existing staff and maintaining custom solutions that do not benefit from the shared economics of industry standardization.

Silos of virtualization with dedicated resources provide the assurance of reliability and performance that CSPs require, but they offer only a fraction of the cost benefits of the new solution. For example, the silo solution does allow the cost to shift from proprietary to commercial off the shelf hardware. While it does allow the on-boarding of new functions more quickly via software, it fails to shift the Operating Model significantly toward automation across the CSP's network.

Entrusting a single supplier to implement NFV/SDN/MANO creates a proprietary lock-in effect where the technical and product lifecycle choices of the supplier dominate the CSP's cost model. This approach limits CSPs from gaining the cost reduction benefits of standardization and particularly limits the value of open source solutions.

Gradually, CSPs are addressing these obstacles with the help of joint initiatives, such as ETSI's Open Source MANO (OSM), Metro Ethernet Forum's Lifecycle Service Orchestration (LSO), as well as initiatives by Open Platform for Network Functions Virtualization (OPNFV), Open Network Automation Platform (ONAP) and Open Network Foundation (ONF). However, these groups are primarily addressing the standardization and complexity of the solution.

They are not yet providing a remedy for the operational model problems caused by a CSP's current operational environment. That mindset is driven by organizations staffed with specialized network engineers who must develop or integrate the skill sets of IT-oriented software programmers.

7 OPERATIONS MODEL CONFLICTS

Most CSP organizations have relied on a Network-Centric Operations Model (shown in the bottom left quadrant of Figure 6) based on a hierarchy of processes that react to network events. The processes are integrated through a series of tightly coupled systems. These systems are integrated north to south from the Business Support Systems (BSS) to the Operating Support Systems (OSS) and eventually the physical network. They are also integrated east to west with each adjacent domain triggering a process in the neighboring domain from the access point to the network edge to the core. These well-engineered networks operate very efficiently by reacting to known events—from a call set up to an IP packet transfer. This makes them highly scalable and reliable for voice and data traffic.

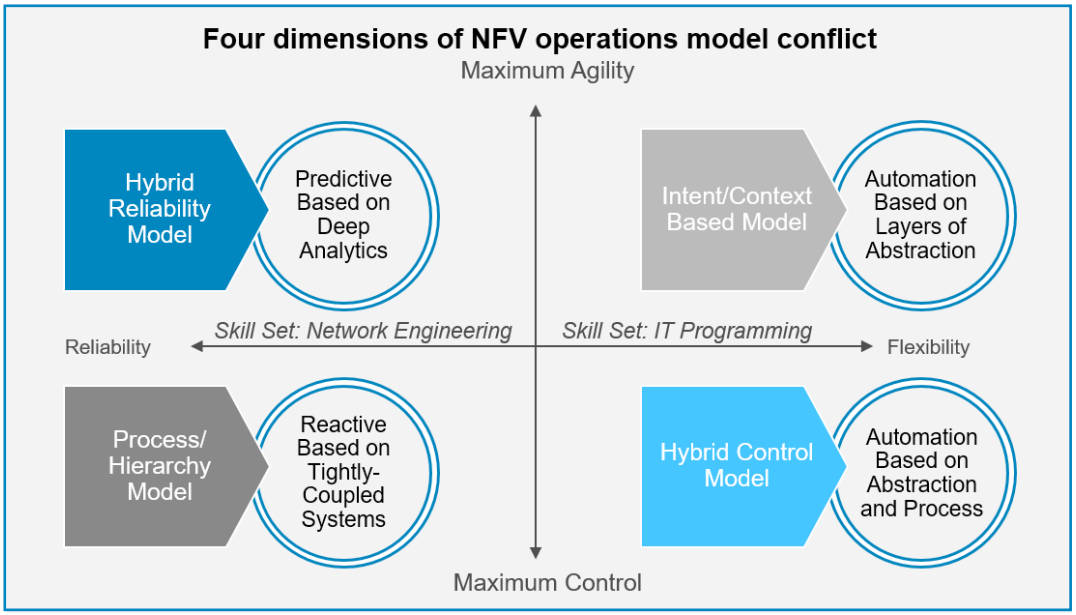


Figure 6. NFV Operations Model Conflicts

However, these networks are more difficult to change, as significant re-engineering and reconfiguration is required to build or redefine processes for new service types or for cross-domain processes. This inflexibility coupled with the cost and slow upgrade cycle of the proprietary systems they were built on is making them too expensive to maintain in light of competition with IT/cloud-based virtualized infrastructure that operate with far more flexibility at much lower cost.

The new Operating Model is often called Customer-Centric because it derives its marching orders from the end customer's preferences and actions rather than internal network processes. The new model is driven by interpretation of the customer's intent within a given context (shown in the top right quadrant of Figure 6). To achieve the high degree of predictive reliability that this intent- and context-based model will require, CSPs will leverage analytics that feed machine learning programs that autonomously adapt the network response to the end customers' needs (these characteristics are depicted in the top left of Figure 6). Controlled scalability, instant provisioning and unified operations are another set of key characteristics of the new operation model. Critical to control are automated processes based on abstracted network layers (shown in the bottom right of Figure 6).

These dimensions are depicted as Operation Model Conflicts because CSPs face a multi-stage migration from the old to the new models, with the need for hybrid approaches along the way and gradual deployment of layers of analytics, abstraction, policy and orchestration before achieving automation. Today, early adopter CSPs have experienced the conflicts of these models, especially when network staff are asked to implement IT frameworks and platforms that lack the fine grained reliability guarantees they expect.

8 CASES IN POINT

The following examples are drawn from early CSP implementations of the new Operating Model. They provide lessons learned and point the way to a new approach that can accelerate deployment.

CSP NFV Failure to Migrate Case

- **Issue**: Country-based network engineering's mistrust of virtualization led CSP to replace IT vendor with network supplier.
- **Result**: Static NFV implementations limiting benefits of virtualization and delaying transformation.

8.1 CASE 1: FAILURE TO MIGRATE

One of the first grand plans to implement the new Operating Model was undertaken by a European-based Tier 1 multinational communications service provider with operations in more than 20 countries (see sidebar). To deliver on its promise to move quickly, the provider created an overlay organization within its CTO office that brought together network and IT experts. After testing the many variants of NFV and MANO in its labs from multiple suppliers, the company selected a single vendor to not only create a common environment within its regional data centers, but also deliver NFVI and MANO within each operating company.

Within the data centers (where IT was in control) the transition to virtualized infrastructure was going smoothly, but in the operating companies, objections began to surface regarding assurance of reliability of the new network elements. Network engineers within the service delivery organizations were accustomed to building out hardware platforms that provided capacity for new services and stitching together processes to assure end-to-end service delivery. These tasks involved identifying tight coupling of physical network functions, such as IMS applications with the necessary storage and server capacity they would require based on traffic expectations. Network engineers were also required to link the control and provisioning systems directly with the functions. While complex due to the number of systems involved, this process was facilitated by software functions that were physically bundled with hardware.

With the introduction of NFV, a new process model was required. The functions became physically separated from the servers and storage they required. The control and provisioning systems that linked the new IMS systems to back office platforms became logical software-based objects abstracted from direct physical connections. For network engineers, this new framework not only challenged their skill sets, but also confounded question such as, "if the function experiences a fault due to a lack of capacity, which server or storage device should we check?" In the network-centric model, dedicated devices make this a question with a straightforward answer. In the new model, the network control mechanisms automatically shift capacity to which ever functions require it—on demand—so there is no physical linkage to dedicated capacity. This environment flummoxed the network engineers.

The operating company network engineers were not comfortable with the virtual environment and ultimately required the vendor to implement a hybrid model where the platform was virtualized for the IMS applications, but the capacity was dedicated to the functions. This satisfied the local company, but created two problems for the vendor and the CTO.

1. The first problem was that each operating company was then able to dictate the configuration it wanted – truly virtual or hybrid or something else and the benefits of virtualization were mitigated with little true ability to automate the CSP network across its data centers and operating companies.

2. The second problem was an increase in cost due to vendor development as well as the requirement for additional dedicated capacity.

3. The end result was that this project failed to deliver the promised benefits and ultimately cost more in customization—including the vendor creating new software implementations—than expected. The vendor was demoted from being the strategic lead on the project and the CSP hired a new partner who was willing to absorb the cost of the different models.

The above hybrid approach has continued to cause delays: taking more than two years to go from trial to implementation. The deployment is still only at moderate scale for targeted NFV services. Like many early adopters such challenges have caused the company to focus on non-critical network elements rather than close to the customer systems. This limits the risk but also mitigates the benefits of the new operating model.

The CSP is still pushing NFV-based transformation and has since advanced to promote industry-standard operating models for NFV that include sufficient assurance measures to satisfy the network side, while including as many benefits as possible from the IT side. Nevertheless the progress has been slower than expected.

CSP NFV Silos Never Die Case

- **Issue**: National Mobile Operator lacked skills for NFV/SDN migration to vEPC.
- **Result**: Vendor solutions lacked interoperability and created silos.

8.2 CASE 2: SILOS NEVER DIE

In another case, a European Tier 2 CSP was determined to move forward with NFV but found that they lacked the necessary skills. (See sidebar.) When they called upon vendor support, the recommendation was to recreate the silos of the past. While the CSP (a national mobile operator), had the network staff with core competency in managing service level agreements (SLA), maintaining network facilities and managing traffic, the company lacked skilled staff in the following areas:

- Experts knowledgeable in the technology of each layer of the virtualization stack
- Core network engineers who understood flow architecture design and management for software defined networks
- Staff who understood the technical requirements of orchestration across network domains
- The experience to eventually implement a new DevOps service delivery model

The CSP hoped to tap into an industry ecosystem of players that were touted in the many NFV lab trials sponsored by ETSI and other organizations. What they found was a stark reality:

1. New suppliers with the technical solution in the lab or in small scale node-based deployments that had yet to deliver a scalable solution in a production network.
2. Large traditional suppliers who could bring the expertise required but only in a solution designed largely around their own products.

With reservations about reliability already present within the network operations group, the CSP could not afford to select an untested small supplier. So the company chose two large suppliers. The operator already had RAN equipment from each and decided to extend the solution to include a transformation of the Evolved Packet Core from each supplier using NFV/SDN technology. Each supplier was also asked to incorporate as much open system technology into the solution so that interoperability would be easier.

What ensued was a jockeying for position and a battle between two-vendor silos. Each supplier used COTS hardware but each had their own virtualized EPC and related applications. But the real conflict came with respect to orchestration. The CSP simply did not want multiple orchestrators, yet neither supplier could provide an effective multivendor solution for orchestration.

Once again the traditional industry mode of multiple versions of proprietary products was blocking the cost savings and automation agility that the new operation model affords. The CSP chose a third-party multivendor orchestration platform instead. However, the solution was based on open source and it required the CSP to add staff experienced in open source orchestration and with knowledge of the virtualization stack to effectively implement and manage the solution.

Eventually, the CSP hopes to consolidate the solutions into a single supplier platform, though the company will likely maintain an open source orchestration environment, which it hopes will continue to mature. The entire process moderated the CSPs enthusiasm for NFV, but it nevertheless has engaged in staff retraining to supplement the skill sets it will need in future implementations. On the horizon, the CSP expects to migrate to more NFV/SDN elements for 5G and small Internet of Things initiatives, hopefully with less silos.

CSP NFV Skepticism at the Top Case

- **Issue**: CXOs thought NFV would fail, despite competitor success, so they delayed deployment.
- **Result**: CSP gradually moving forward, year or two behind competitor, but still no organization shift.

8.3. CASE 3: SKEPTICISM AT THE TOP

The idea of failure, fast or slow, is anathema to CSP executives, yet the new Operating Model requires a change in that mindset (see sidebar). One large North American Tier 1 CSP confronted exactly that problem when the IT and Network Operations departments agreed that they were losing ground to a close competitor who was implementing NFV/SDN/MANO in a broad strategic project, while their own company was mired in tactical trials.

The CXO team simply did not believe the hype and were looking forward to the inevitable cost overruns and public failures it believed that the competitor would ultimately experience. Their objections included the fact that while the loss of a virtual function in a small scale trial would not be noticed, the failure of a large scale initiative could easily knock out 50% of the CSP's services. They did not believe that a well-architected and orchestrated NFV infrastructure would be as resilient as the traditional network.

So instead of going forward with a strategic campaign of transformation, the CSP adopted a conservative approach. It deployed NFV using gradual steps, one node at a time, first in some core elements and at the network edge. Each NFV stage was broken down into small increments and each increment was unit tested, module tested, regression tested, performance tested and scale tested.

While the executives liked the idea of cost savings by separating the software and hardware procurement cycles, they were unclear on balancing internal and external operational spending—for either hiring more systems integrators versus hiring and training internal teams or a blend of both.

So the department teams took it upon themselves to shift to the expertise necessary to prepare for the transformation. They encouraged the Linux factions within their organizations to advance trials of open source solutions and participate in industry standards groups.

The result was a broad retraining program and eventually a costly shift away from a traditional Operating Model to more and more distributed nodes orchestrated through a common platform. Grudgingly senior management accepted the change, especially when the competitor did not fail. In fact, it was the competitor's claim of their incremental revenue from NFV/SDN and substantial long term cost savings expectations that led the CSP to follow suit with an aggressive SD-WAN roll out and announcement of distributed virtualized edge network nodes.

Today there is a formal retraining program and an ongoing transformation of functional domains at the CSP. However, the CSP is still a year or two behind its competitor and has yet to launch a company-wide strategic goal of total conversion to the new model.

Part of their challenge was more organizational than technical. The CXO team was not ready to extend the influence of IT and CIO departments across network operations, even though the underlying teams were already working together on the trials and new initiatives. Similarly, the CTO did not want to shift the purview from operational to future focus, making room for the IT team to increase its operational influence. These perspectives and 'battle lines' are common in early adopter cases at CSPs.

9 ACCELERATING NFV DEPLOYMENTS BY BRIDGING THE IT/NETWORK OPERATIONS GAP

9.1 OVERVIEW APPROACH

As detailed in the prior sections, there are many challenges to accelerating NFV deployment and overcoming operational obstacles. At the core, the challenges are not limited to the adoption and integration of the complex solution stack—but also include people and process changes needed to be successful.

Dell EMC has developed a comprehensive NFV infrastructure portfolio that simplifies, accelerates and de-risks NFV adoption. This portfolio includes a set of proven reference architectures, the Dell EMC NFV Ready Bundles for both VMware and OpenStack, offering customers a fully engineered, tested, validated and supported NFV infrastructure, a great starting point for developing a Telco cloud. Dell EMC Ready Bundles are open and provide customers with choices across the technology stack. These virtualization choices, combined with a range of SDN controllers, Dell EMC Service Assurance, and management & orchestration, coupled with a full range of services round out the portfolio.

Dell EMC's consulting team has engaged in more 2000 successful enterprise cloud and hybrid cloud implementations and has deep experience in tackling the challenges in implementing NFV technology in major CSPs around the world.

Experience with NFV implementations, coupled with our deep heritage in enterprise cloud technology implementations, has shaped an approach for addressing the many challenges found during NFV implementations. While the technology itself can be considered to be progressing, many aspects are not well advanced or stable, including the particularly vexing challenge of end-to-end orchestration. In addition, the 'softer side' of implementation is often the root cause of significant problems. Specifically, the following aspects must be addressed to enable successful NFV implementations:

CSPs must recognize that Network and IT Operating Models have some significant differences:

- Different resiliency mechanisms (node-based versus network-based)
- Different workloads/applications—CSP implementations tend to require stateful, long duration, distributed (vs. Enterprise workloads/applications)
- Different regulatory requirements
- Different ecosystems needing to be integrated (OSS/BSS vs. ERP)

CSPs must acknowledge that there are also economic downsides to having separate Operating Models:

- Specialized headcount ("domains of experts") in both IT and Network
- Accelerating depreciation cycles
- Application proliferation
- Lack of leverage/synergies across infrastructure

Dell EMC's consulting approach specifically addresses the above conditions and provides a framework for realizing success. A new rubric and framework for a combined operating model is the key.

Below is the Dell EMC Services portfolio that can be leveraged to support Network Function Virtualization infrastructure (NFVi) deployments:

- **Dell EMC Network and Services Virtualization (NFV/SDN) Workshop**—Dell EMC NFV/SDN workshop is intended to help customers who are starting their cloud transformation journey to develop a comprehensive NFV adoption strategy. It helps customers prioritize the use cases based on business drivers, understand the technology and platform choices such as VMware, Red Hat, etc., identify infrastructure virtualization opportunities, develop strategic roadmap for implementation phases. This includes understanding current state, understand requirements, GAP analysis and collaborative services to define technology, process implementation paths to ensure successful transformation.

- **Dell EMC Network and Services Virtualization (NFV/SDN) Business Advisory**—This service is intended to help customers develop a business case to adopt NFV based business drivers. It helps demonstrate to senior management the benefits of moving towards a shared NFV cloud infrastructure. This includes an independent and collaborative review of the business objectives to develop a comprehensive business case for the transformation including the Total cost of ownership/Return on Investment financial model.

- **Dell EMC Network and Services Virtualization (NFV/SDN) Proof Of Technology**—This service is intended to help customers quickly prove out the desired technology stack and get some hands on experience with the NFV infrastructure. This also helps customer evaluate technology choices to develop plans for production deployments. The service includes on-site infrastructure assessment, deployment and testing of an NFVi proven platform in a non-production environment. Planning, implementing and onboarding of NFVi and VNFs in a laboratory environment is also included.

- **Dell EMC Network and Services Virtualization (NFV/SDN) Implementation Services**—Dell EMC NFV Ready Bundles offer a risk free option for our customers. To ensure faster time to value Dell EMC Implementation services provide on-site infrastructure planning, implementation, onboarding and orchestration of NFVi and VNFs to a production environment, for both custom infrastructures and Dell EMC NFV Ready Bundle customers. This includes Operating Model development and implementation, process refurbishment, blueprinting and technology implementation support.

- **Custom Consulting Services**—In addition to the services described above, Dell EMC has many custom services that provide advice to customers on transforming data centers, infrastructure, applications and operating models to take advantage of cloud, Big Data, Internet of Things (IoT), mobility and security.

- **Managed Services**—Using well-defined processes and innovative tools, Dell EMC provide end-to-end management and optimization of customer NFV environments, allowing them to reduce operating and support costs while efficiently maintaining and administering applications within agreed service levels.

- **Support Services**—Our highly-trained experts provide comprehensive hardware and software support. Our industry-leading proactive and predictive automated tools, flexible response options and multiple support channels help prevent downtime, increase IT and end user productivity and reduce effort, allowing customers to shift focus from day-to-day maintenance to innovation.

- **Education Services**—Our training and certification offerings enable clients to transform people and organizations to maximize the value and impact of Dell EMC products and solutions and position IT as a trusted advisor to the business in the digital enterprise. We provide organization-wide access to development and certification opportunities that span IT Services, Processes and Infrastructure Management, Cloud, Big Data, DevOps, Dell EMC Products and more, delivered through a variety

of in-person and on-demand learning methods. Our training and certification programs are designed to ensure our clients can acquire, develop and retain talented IT professionals.

Dell EMC has a collaborative approach to projects that can be summarized as a 'do with' rather than 'do to' approach and has considerable experience in enabling enterprises and service providers make the transition to the cloud. This includes traditional cloud enablement like private/hybrid/public cloud as well as telco cloud enablement with NFV/SDN.

The following sections describe our approach to each of the prior case studies to accelerate NFV deployment and achieve CSP operational excellence.

9.2 OUR APPROACH TO CASE 1

To address the challenge of migrating away from silos to a new NFV architecture, the Dell EMC approach starts with the ETSI NFV Model, which specifies that a typical Network vendor "appliance" be separated into its component parts:

- **Infrastructure (NFVi)**—Compute, storage, networking
- **Network function (VNF)**—Application layer to provide customer configuration and execute the network function
- **Management software (Mano)**—Allows operation and management of the layers

Separating an appliance into parts enables the virtualization of the network function similar to the way in which IT applications have been transformed over the past 10 years to run on standard hardware platforms, giving the application owner the ability to focus on the application features and less on the hardware components. This technique drives significant cost and speed benefits to the end consumer, provides more business agility and can be monetized quicker than by implementing a traditional network function provider proprietary stack.

Most IT organizations have depended heavily on virtualization for years and have evolved their processes into providing their business units with Infrastructure as a Service (IaaS) where business units can consume, via a standard service catalog, the necessary infrastructure in a self-service, on-demand basis. The next evolution where mature organizations implement best practices is to create an IaaS Service Center in which to manage the 1) consumer demand for new infrastructure services, 2) modifications to existing services, 3) build of new services and the 4) operations of the new services with a continuous feedback loop. This same IaaS technique can and should be applied to NFV implementations.

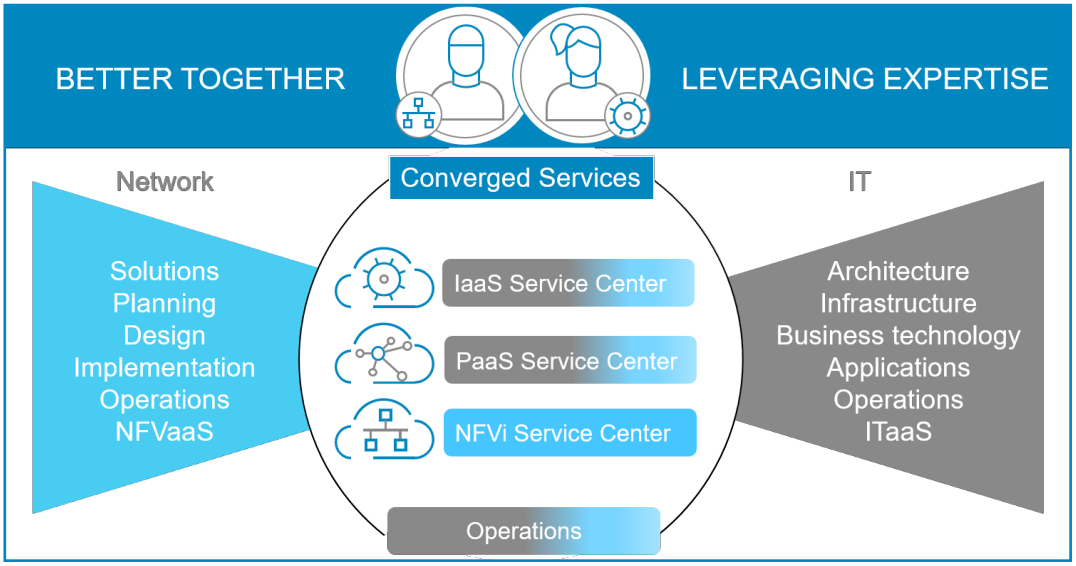


Figure 7. Dell EMC's Agile Service Center Organizational Model

As IT organizations mature, they advance the IaaS concept to include software components further up the stack that can be standardized across the organization to achieve faster deployment, reduce maintenance effort and reduce operational complexity. The additional of software components to the Services catalog in the same way as IaaS is known as Platform as a Service (PaaS) and from a best-practice perspective is managed in the same Service Center approach as IaaS. The skills required in the PaaS Service Center are more application middleware, database, messaging and software based in order to manage the demand, implementation and operations of the PaaS services. With both the IaaS and PaaS Service Centers providing standard pre-defined components on a service catalog, the end consumer of these services realize an agility benefit by reducing the time to design, request and provision of services from months to days and sometimes to minutes.

With the adoption of NFV by the CSPs, there is a need to move from conventional network vendor dependence to an open approach where the customer is centric to the decision of which Virtual Network Function (VNF) to deploy. This will be driven by the ability to launch new services that drive new revenue streams or reduce the cost to deploy and maintain previously unwieldy network vendor appliances. The main challenge for the Network organization is that it will need to adopt new business processes and acquire critical virtualization skills to manage the components (as defined by ETSI) such as NFVi. These management skills are readily available in most IT organizations and often are under the control of the same CTO.

In order to achieve the highest leverage of the organizations assets and capabilities it is recommended that a NFVi Service Center, similar in process and design to IaaS and PaaS, be created to manage the 1) consumer demand for new infrastructure services, 2) modifications to existing services, 3) build of new services and the 4) operations of the new services for needs of VNF's. The NFVi Service Center would leverage previous investments made by the IaaS and PaaS teams in order to avoid recreating the wheel in terms of expertise and services.

To truly transform a CTO's organization to optimum efficiency to compete in customer satisfaction, service agility and cost management a converged team be built that leverages the strengths of both the Network and IT organizations. This new 'Agile Service Center' organization model that leverages the strengths of the Network and IT organizations is outlined in Figure 7.

The first step in the Dell EMC consulting project is to review the above model as a 'straw' model using facilitated workshops with both IT and Network executives and resources. This participatory approach is key to understanding current long standing beliefs within both the IT and Network organizations. Furthermore, the participatory approach allows executives and resources to design an organizational model that is 'right' for the CSP.

The second step is to take time to review the proposed organizational model with all stakeholders, from executives down to all team members at every level. This participatory review will certainly elicit comments and will help ensure all team members feel 'a part of the process'.

The final step of the approach is to develop a phased implementation roadmap which includes all aspects of proposed changes. This step includes holistic ROI modeling for the entire NFV initiative including implementing the new Operating Model. Our experience is that frequently CSPs develop ROI models solely based on technology implementation costs and neglect the costs of transitioning to a new Operating Model. Our final presentation includes the following topics:

- Strategy Definition for Organization Change
- Current State Maturity Assessment
- Future State Service Center Organization Design

- Metrics and related Analytics for Service Center Organization
- Implementation Roadmap to achieve Organizational Maturity and New Structure
- Financial ROI Analysis of Process and Organizational Benefits

In conclusion, had the carrier identified in Case 1 adopted a similar organization design it would have had a structure where all virtualization skills existed with well-known and published support processes that the organization could leverage instead of the many operating companies questioning, rethinking, fearing network virtualization and ultimately failing to migrate to the new Operating Model. NFV will create the opportunity for many carriers to be successful to the degree in which they are able to adapt their organization to the available technology, processes and organizational change needed to compete. Dell EMC has the expertise and experience to help carriers achieve this organizational change.

9.3 OUR APPROACH TO CASE 2

Seeking multi-vendor support to deploy NFV initiatives for organizations that lack the appropriate skills, coupled with the concept of leveraging open source technologies and an ecosystem of partners in order to kick-start these initiatives is great in concept. Where we saw the European Tier 2 CSP falter was in looking solely to traditional network vendors to help them solve the above. Traditional network vendors are inherently interested in protecting their perceived “turf” and will look to deploy virtualized applications and infrastructure that, while perhaps aligned to the ETSI, prove to not be interoperable.

NFV transformation has three major implications, all of which are related:

1. It requires the organization to adapt to a new way of working (and thinking) about how to deliver these business models to end users. This is helped by tool sets and integrated environments that span across physical, virtual and application layers.

2. It enables new service provider business models, opening up new revenue opportunities and ways of consuming services.

3. It drives a new technology architecture that is more efficient, scalable, dynamic and cost-effective.

The NFV Operating Model can be much more efficient than traditional ways of managing the infrastructure, but it requires a different way of thinking and structuring of the technology (network and IT) organizations. Previously the network was built and managed and services needed to be applied to existing infrastructure/capacity constraints. With SDN and NFV we now can map supply of capacity much more effectively with demands for workloads and do it in a dynamic way that is capable of adapting to unpredictable and varying traffic patterns.

The Network Function Virtualization Infrastructure (NFVi) represents a programmable HW “substrate” that can support compute, storage and network resources that adapt to the demand from a variety of end-user and infrastructure virtual functions and are networked and scaled through SDN control plane abstraction. At Dell EMC we have deployed some of the largest NFV deployments in the world, including the largest Open Stack IaaS deployment—serving up a common set of infrastructure and tools where providers can deploy their VNF applications. We believe that a composable architecture that allows for the Management and Orchestration layers to mediate between application requirements (whether Open Source or VMware) is key and makes deciding on a platform less critical and more on the applications that will be driving new sources of revenue.

The key for CSPs is to decide on the platform and then work with a company that will help them onboard required VNFs to test and certify on the underlying infrastructure, integrate these into OSS/BSS functions and deploy for POCs. In order to avoid perpetuating technology and organizational silos, a consultative process with involvement by CSP executive management should be used to bridge and integrate technology, process and operational silos. It is precisely this consultative approach is a core component of Dell EMC Services.

9.4 OUR APPROACH TO CASE 3

This case is less of an IT and Technology problem versus what we could traditionally consider a management consulting problem. Perhaps there was a lack of an alignment between the business and technology groups in how a transformation to virtualized services could accelerate business cycles and improve profits (not just savings). This is very typical. The last paragraph stated the problems very clearly—"their challenge was more organizational than technical."

Organizations need to get behind their technology transformations and transform their organizations to best support the new technology and business models. Setting up shared organizational service centers across network and IT operations (Figure 7) reduces the possibility of failures caused by the power struggles seen in organizational silos—and allows teams to work together and best serve the business on the trials and new initiatives.

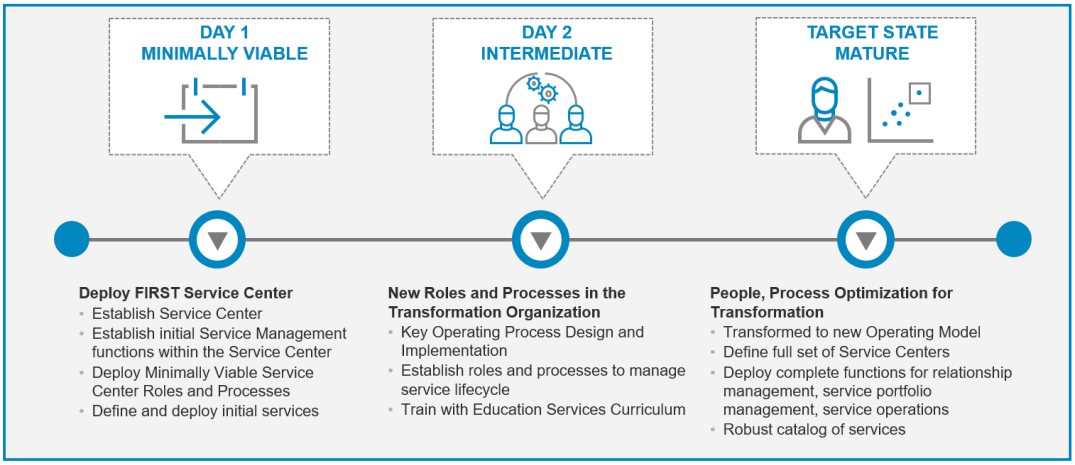


Figure 8. Dell EMC's Transformation Approach to Deploying NFV Agile Service Centers

Similarly, the CTO did not want to shift the purview from operational to future focus, making room for the IT team to increase its operational influence. These perspectives and 'battle lines' are common in early adopter cases at CSPs.

Dell EMC has considerable experience in enabling enterprises as well as CSPs to make the transition to the cloud, which is highlighted in Figure 8. This includes traditional cloud enablement like private/hybrid/public cloud as well as telco cloud enablement with NFV/SDN. It is precisely this experience that is extremely relevant for CSPs deploying NFV technology.

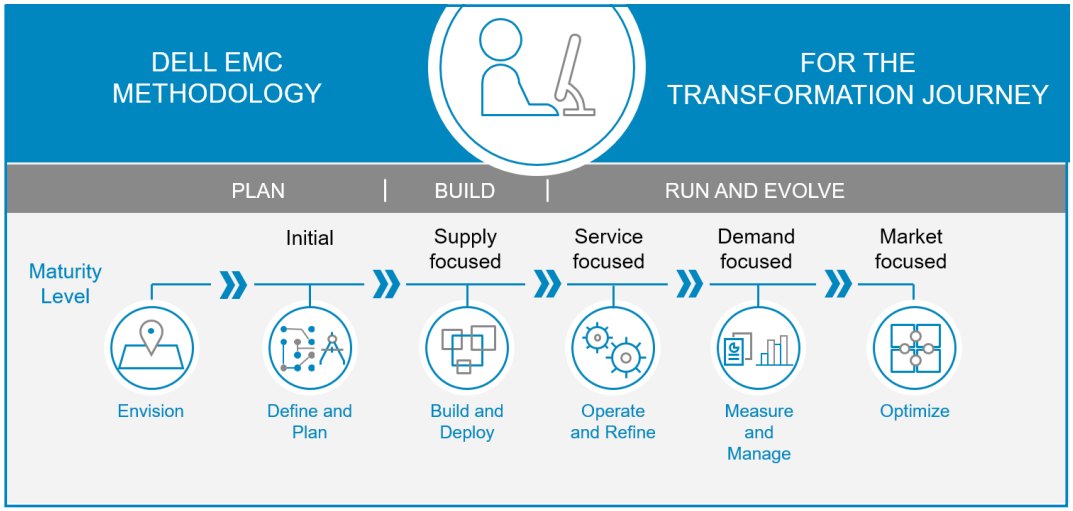


Figure 9. Dell EMC's Methodology for Transformation

Had this North American Tier 1 CSP been our customer, we would have started off the process (see Figure 9) by showing the C-level suite the opportunities ahead of them through a Business Case/ROI analysis—using financial modeling to help the operator quantify the benefits of NFV and SDN as technologies and also quantify the additional benefits that can be accrued from deployment of specific VNFs.

The advantage of this type of analysis is that it can range from high level, single VNF analysis to very detailed and multiple-scenario modeling with sensitivity analysis and model the exact specifications of an individual service provider—their network, their service portfolio and their end users.

Additionally, in order to set the CSP along the right path, we would have recommended an assessment of the client organization across strategy, Operating Model, process, technology and infrastructure and drill down into the key capabilities required for NFVi management. We would then leverage this assessment to define the mission statement, project charter and KPIs for the transformational initiative.

It is key to understand where each client is coming from in terms of their existing organization and what the target goals are in order to get to the Future State operational model. No one “right” answer is applicable to all CSPs and transitioning to an NFVi Operating model will require tradeoffs.

The Dell EMC best practice recommendation is to adopt a Service Center approach to be the single point of focus for the definition, creation and implementation of new services, as shown in Figure 7.

The key areas are defined here with basic functions in each group necessary to understand demand from the business and translate that into providing a consistent and agile approach to delivering service capacity. Obviously there are challenges to shifting an operational model. First, agility cannot abandon quality; what this means is that the effective speed to deployment of a service is always gated by the slowest component of the deployment process, which is usually the Test/QA process. As we noted in the case above, the dev test process itself is one of the biggest barriers to achieving agility in the organization’s attempt to gate restrict and control the quality of solutions being offered to market.

Typical telco service deployment processes are generally based on waterfall software development lifecycles and now need to transition to an agile/continuous Development and Operations (DevOps) process under the following guidelines:

1. It needs to evolve from highly manual process to an automated one.
2. It needs to be able to handle complex infrastructure that represents actual end-to-end service deployments.
3. As part of the governance, a loop of continual improvement must be set up in order to have feedback from all aspects of the service into the process to improve both current and future services.

Dell EMC has significant, relevant experience in modernizing software development processes and implementing DevOps processes within their IT organizations. Nearly every customer that we talk to is trying to solve the above same basic challenges. How can I go faster? How can do it without compromising quality? How can I use this change to reduce technical debt (complexity)? And, how can I do it so that costs are positively impacted? In short, how can I go faster, better, for less cost? Our DevOps experience directly translates to help CSPs implement modern processes for NFV implementations.

A roadmap and vision is critical to ensure that solutions being built are aligned with corporate objectives and designed to scale past the specific needs of single team. This vision comes from the leadership team and provides the context in which the DevOps transfor-

mation takes place. The approach or the act of building actual elements of the solution come from the bottom up. Employ the expertise from the trench to design and develop the solution in accordance with the vision or the "what." This helps with adoption as the users of the system helped to design and build it and translates the vision into measurable outcomes and goals to drive the design and build, as outlined in Figure 10.

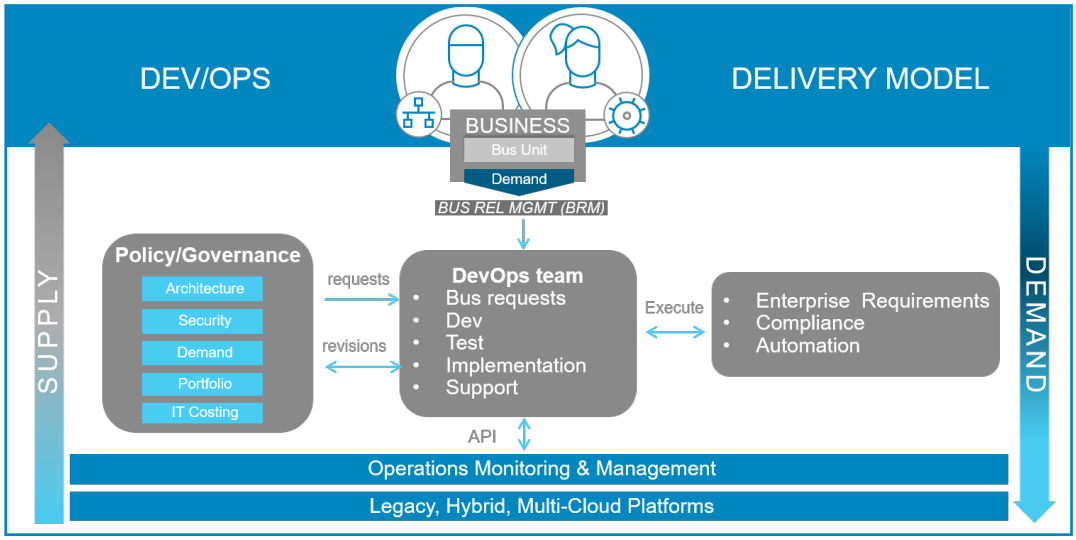


Figure 10: Dell EMC's DevOps Operating Model

Key takeaways in the transformation to DevOps:

- Create dedicated, cross-functional teams consisting of key stakeholder from across the development and deployment value stream. This should include developers, testers, infrastructure, build management, security, compliance, etc. And remember, design and build team aren't required to be the same. It is more important to have all stakeholder present in the design even if only a subset actually build. As you mature in this process, many of the activities your initial build team do will become part of the development process and a key acceptance criteria for new features.

- Delivery pipelines manage the process of a change moving through the various stages and quality gates of your SDLC. In short, they are the automated workflow that mirrors your build and deployment practices and the framework and API architecture that enables you to add tools as they become available. In early iterations, you will be limited by many of the existing constraints that are motivating you to transform in the first place, like long builds, no automated testing, etc. As your pipeline and processes matures new tools are added, new practices are engrained and the pipeline accelerates.

- Focus on automation and tooling.

- Measure your results—release frequency, mean-time-to-change, mean-time-to-recover or time-to-first Production defect are all metrics that can illustrate the health and performance of your delivery pipeline.

- Before starting your transformation baseline your current performance. Then make changes and re-measure so you can learn what works and what doesn't. More importantly, numbers are the language of executives. Without metrics, it is very difficult to demonstrate success and/or gain that support and investment needed to transform at scale.

10 CONCLUSION

There is no “right” answer in planning and implementing an operations model for NFV technology—all decisions and options involve trade-offs. The best approach is to ask “what is the right approach for my company right now?” The most appropriate way to determine this answer is via a custom consulting engagement for the CSP to help it determine the most suitable for itself.

Multiple viable options can exist—depending on the current state of operations in both IT and Network organizations. It is only through a careful, independent assessment of the current state(s) of each respective organization can an appropriate ‘way forward’ be developed.

It is critical to balance structural changes and accountability with process efficiency. An appropriate recommendation for this balance can be developed only after an independent review of the culture and environment present within the CSP.

Choices don’t have to be permanent. It’s ok to design a roadmap that is an evolution rather than a flash cut and/or radical answer which may further harden divisions between Network and IT organizations.

Dell EMC’s consulting organization is well positioned to act as an advisor to CSP executive management. Our approach is to help CSPs navigate through the myriad of choices and, together with heavy involvement by CSP management and team members at all levels, determine the most appropriate model for the CSP.