MARKET PERCEPTIONS FOR TELCO SaaS DEPLOYMENT MODELS

Nelson Englert-Yang, Industry Analyst
Dimitris Mavrakis, Senior Research Director

ABIresearch THE TECH INTELLIGENCE EXPERTS™ NOKIA

CONTENTS

INTRODUCTION

Software-as-a-Service (SaaS) is designed to simplify network operations without burdening Communication Service Providers (CSPs) with the risks and costs of network overhauls. SaaS delivers ready-made solutions on a modern, simplified infrastructure with forecastable expenditures, meeting both demands for technical simplification and financial clarity—key benefits that CSPs are not experiencing through the usual fragmented, self-integrated approach. On the other hand, CSPs want a sure-footed investment in SaaS, and as an entirely new delivery system, the market has not fully embraced SaaS and remains skeptical about its capabilities.

This survey research has been conducted to understand the market perception surrounding SaaS deployment models for the core, analytics, and security. A panel of expert respondents and decision makers working for operators were asked detailed questions. The following section describes the survey in more detail.

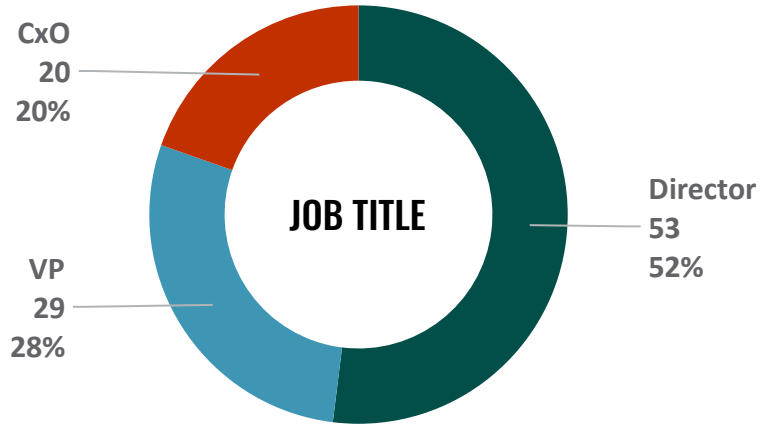
DESCRIPTION OF SURVEY

The survey sample size is n=103, split between operator executives across the United States, the United Kingdom, Canada, and Western Europe. The following sections describe the survey respondents in more detail.

Respondent job titles are distributed as follows:

Figure 1: Survey Respondent Job Titles

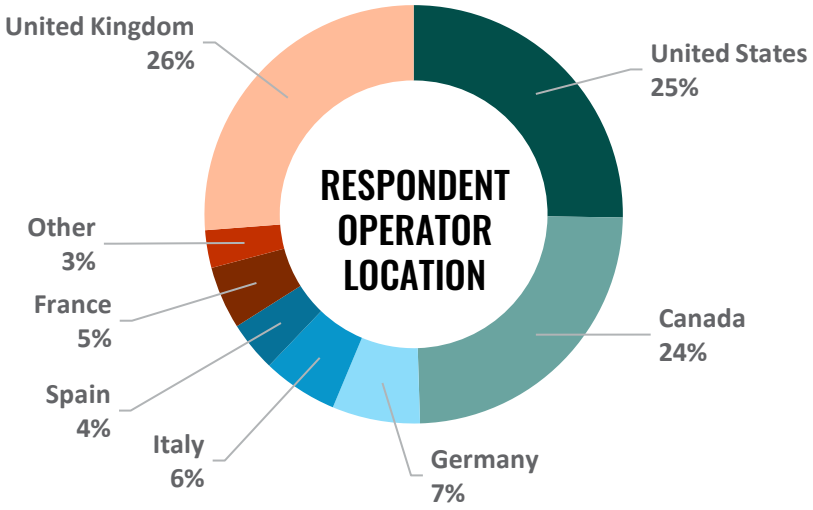
Source: ABI Research



In terms of geographical location, Figure 2 summarizes the survey distribution.

Figure 2: Survey Respondent Operator Location

Source: ABI Research



In terms of geographical location, Figure 2 summarizes the survey distribution.

SAAS MARKET OVERVIEW

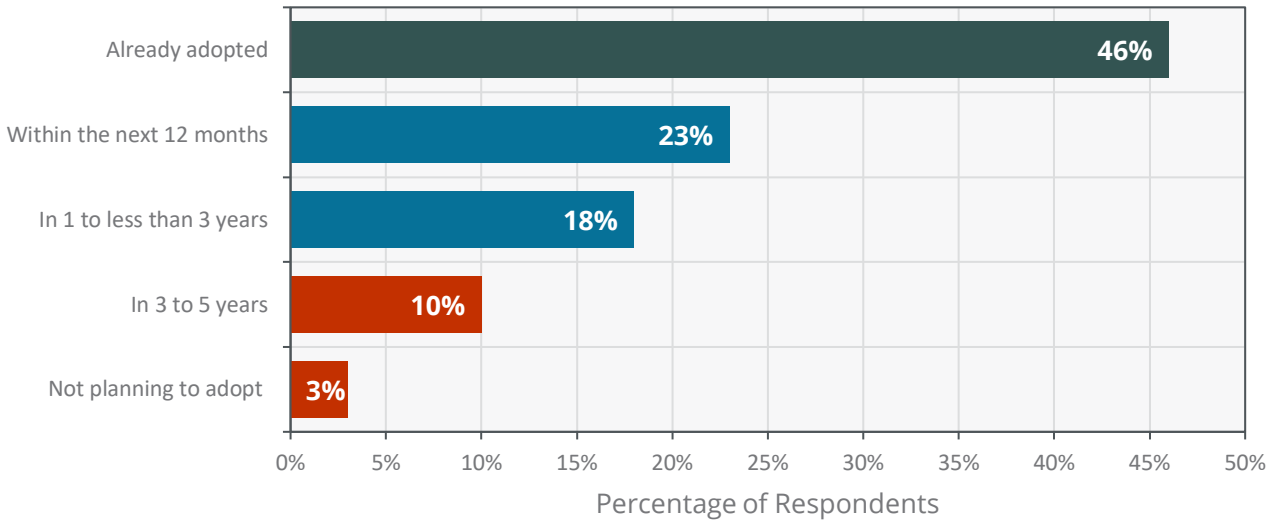
The telco SaaS market is not a uniform domain, as operators may have different approaches and requirements when considering core, analytics, or security deployments. The following sections provide a glimpse into these domains and how survey respondents answered these questions.

MARKET OPPORTUNITIES FOR SAAS

Several survey respondents claim to have deployed SaaS already. Figure 3 illustrates the answers to this question.

Figure 3: How Soon Do You Expect Your Organization to Adopt SaaS Models for Network Elements?

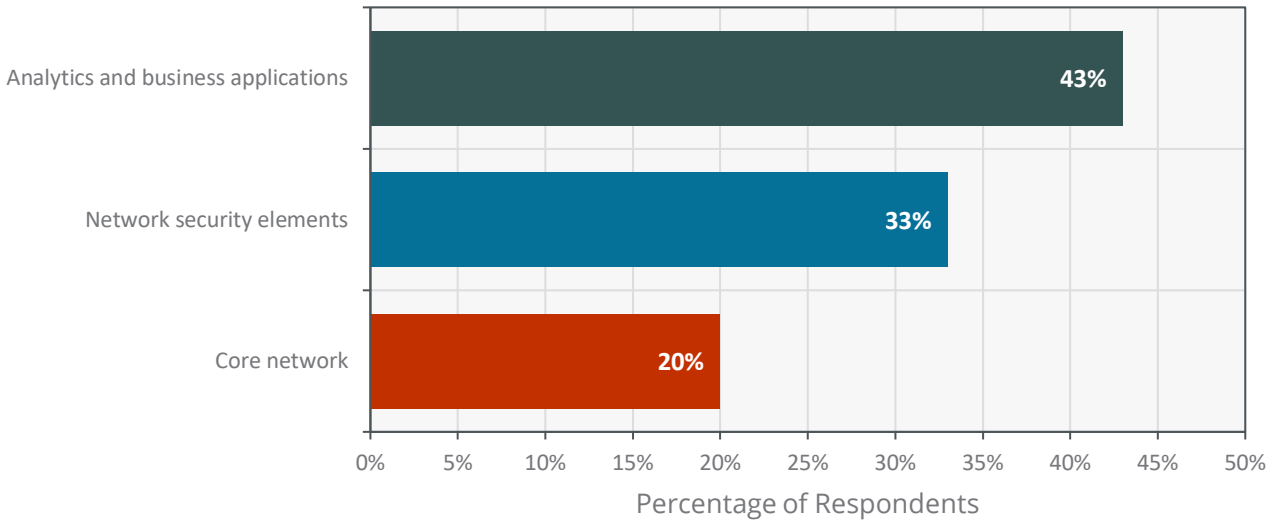
Source: ABI Research



Most operators are expecting to deploy SaaS in the next 2 to 3 years, whereas many operators claim to have already deployed SaaS, most likely in the higher layers of the network stack, predominantly for Operations Support Systems (OSSs)/Business Support Systems (BSSs). The following survey question validates this point.

Figure 4: Which Network Elements Would You Consider Moving to a SaaS Model First?

Source: ABI Research



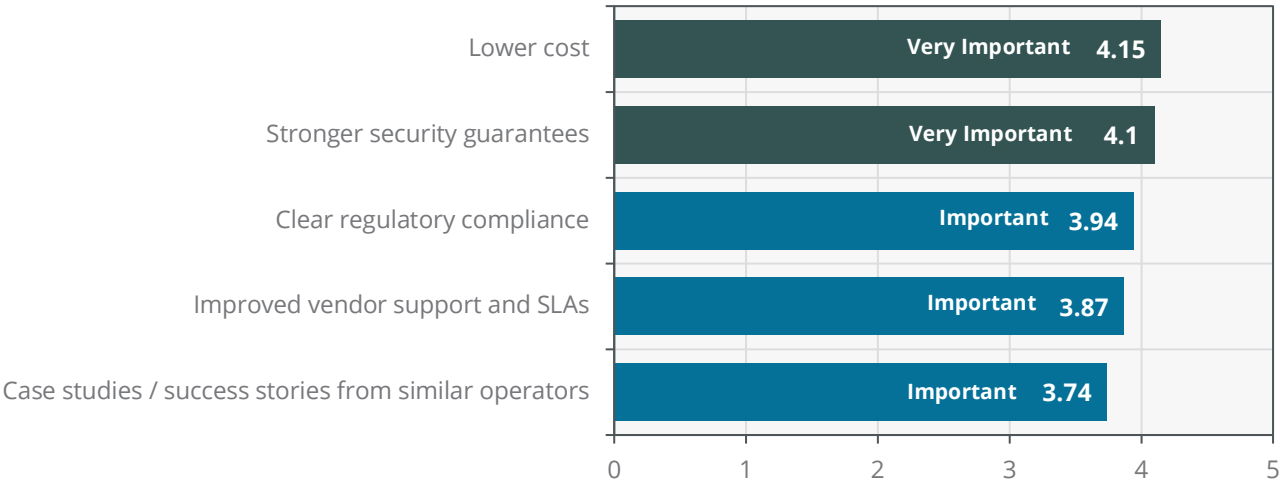
Most respondents are considering analytics and business applications for SaaS deployment models, because these functions are most likely deployed in Information Technology (IT) environments and may not be in network-critical areas such as the core network.

SAAS ADOPTION DRIVEN BY THE PROMISE OF SECURITY AND COST-SAVINGS

Security and costs are top concerns for CSPs' network management strategies. This is true for both their current network deployments and carrying over into their concerns for adopting SaaS network elements. Security and costs were identified as more significant than all other factors in deciding whether to adopt a SaaS model. These concerns outweigh success stories from similar operators, regulatory compliance, and improved vendor support and Service-Level Agreements (SLAs). On our scale from "not important" (1) to "very important" (5), these alternative factors had an average of 3.8: they neither weigh heavily on decision-making, nor are they insignificant. By contrast, both cost and security were above the 4.0 marker, considered, on average, "very important." This identification of security and costs as the top concerns for moving to a SaaS model is the strongest finding in the study, and it is not merely descriptive of the sample, but we find it to be generalizable (i.e., statistically significant and robust compared to samples of other operators).

Figure 5: What Factors Would Accelerate Your Decision to Adopt SaaS for Network Elements? (1=Not important, 5=Very important; n=103)

Source: ABI Research

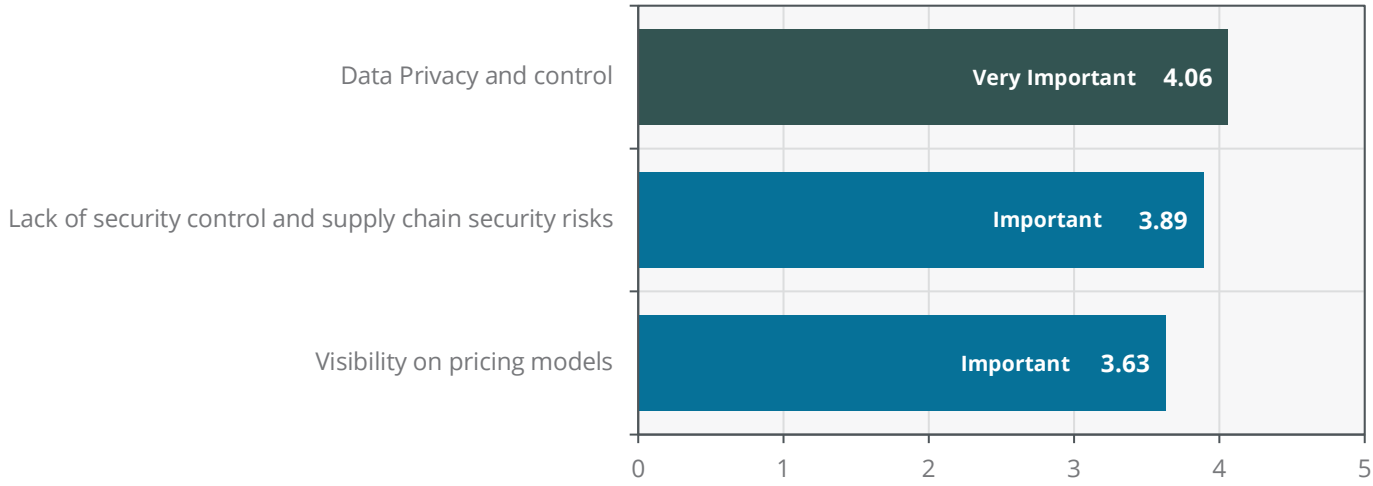


The telecoms industry handles sensitive data across networks of enormous scale and operational complexity, so security and costs are common concerns across CSP software and infrastructure choices—from considering Operational Expenditure (OPEX) on public cloud platforms to making micro-level choices about third-party plugins. In that limited sense, the finding is unsurprising. However, CSP concerns in these areas will vary across different software or infrastructure components under consideration, so SaaS providers should be aware of what costs and security issues matter for SaaS models when targeting CSP concerns. For instance, a top cost concern for CSPs with physical network infrastructure is energy costs associated with data center operations. However, this would not be a top concern under a core network SaaS deployment model where data center operations would largely be outsourced to the SaaS provider. It is, therefore, essential for SaaS providers to identify the specific factors underlying CSP concerns in order to address how these issues are best handled under their solutions. We have identified the underlying factors for this sample of CSPs.

CONCERNS FOR SECURITY, DATA PRIVACY, AND TRUST

Figure 6: Rate the Below Concerns About Security When Considering a SaaS Model Versus a Traditional On-Premises Model for Telco Services (1=Not important, 5=Very important; n=35)

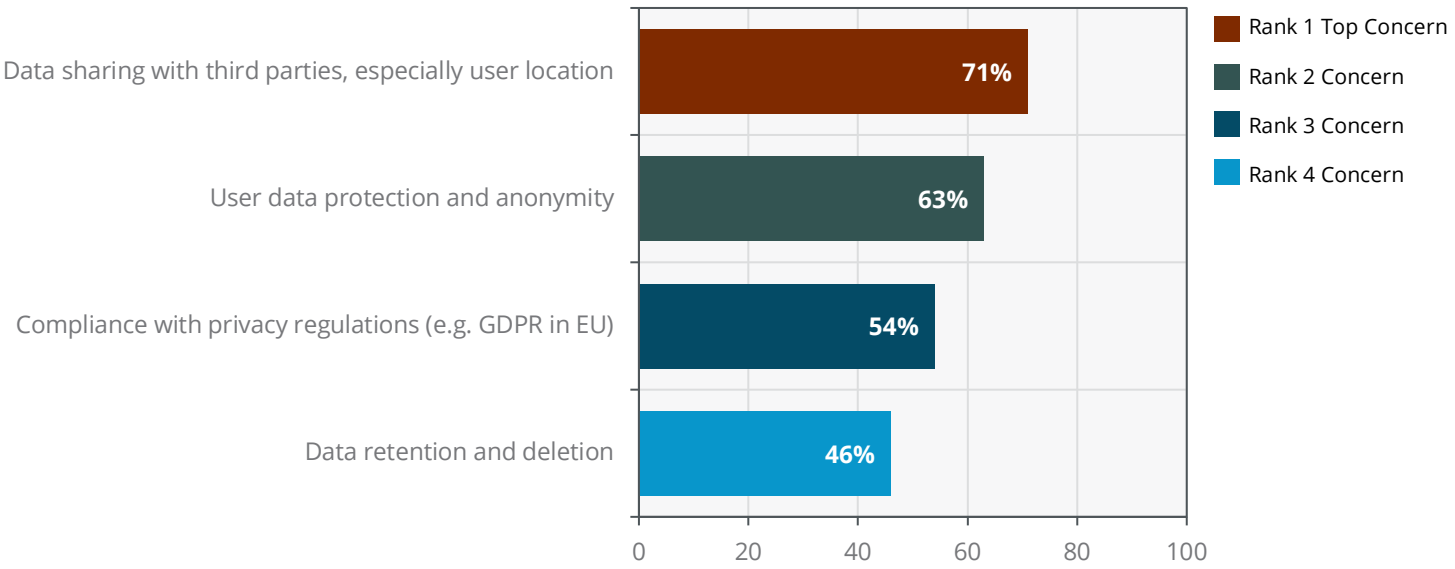
Source: ABI Research



For security, CSPs' primary concern is data privacy. The worry is that data flowing through SaaS providers' managed servers may end up in the wrong hands. CSPs are especially concerned about vendors sharing location data with third parties or violating user data protections. By contrast, giving up security control was important (3.8), but not as important as data privacy (4.0). Overall, the perceived risk that SaaS providers may share data with third parties makes the security issue, first and foremost, a basic trust issue for the CSP, not a technical issue.

Figure 7: What Are Your Top Three Concerns About Privacy When Considering a SaaS Model for Network Security Applications? (0=Not top concern, 1=Top concern; n=35)

Source: ABI Research



SaaS providers should be clear about data-handling policies and procedures, while highlighting experience with telco data. If providing SaaS through the public cloud, providers should reassure CSPs of their trustworthiness through compliance with telco security standards and earned certifications. These two measures were specifically recognized as lending trustworthiness to

SaaS providers when delivering network analytics software. Overall, CSPs want to know that SaaS providers are taking concrete steps with data privacy and compliance. Merely formalizing roles and obligations, as through a shared responsibility model, does not provide the confidence needed by CSPs to deploy SaaS.

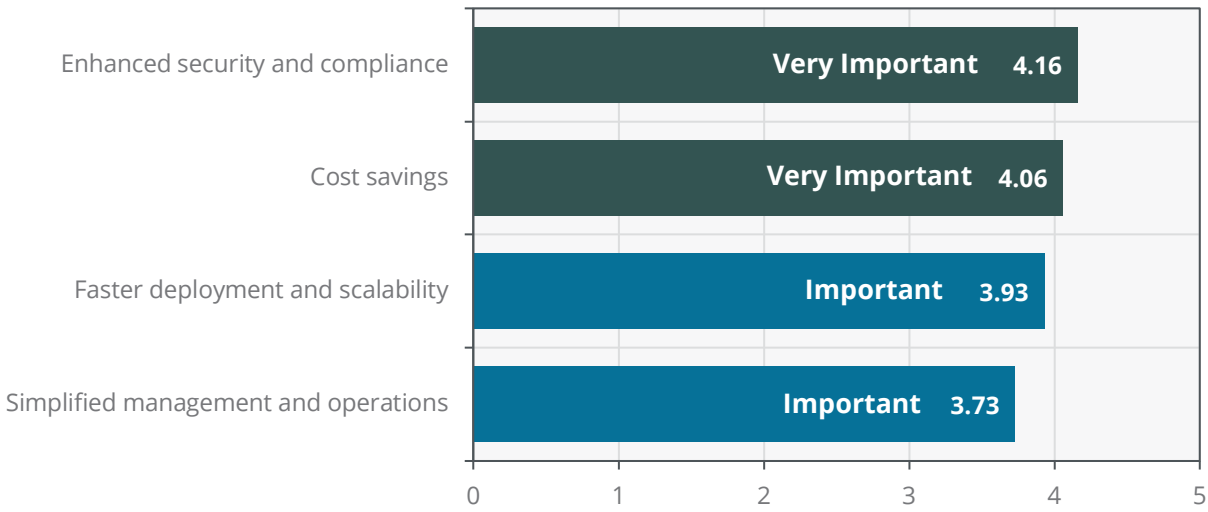
The best way to address SaaS security concerns is by building trust; however, there are supportive technical factors. Strong encryption of telco data is a welcome additional measure for CSPs in case data do end up in the wrong hands, especially when using public cloud infrastructure. Factors deemed insignificant in this context are data sovereignty, multi-cloud hosting, backup and recovery procedures, and incident response.

CONCERNS FOR COST-SAVINGS

Cost is the second key factor, especially for delivery of the network core as SaaS. CSPs are facing extraordinary cost pressures arising from the expense of the 5G Radio Access Network (RAN), which shifts a large burden of cost-savings and efficiency measures onto the core network. CSPs are already widely retaining the 4G Evolved Packet Core (EPC) in a Non-Standalone (NSA) architecture as one cost-saving measure. Beyond this, CSPs must choose to either maintain legacy physical infrastructure or invest in cloud infrastructure with the hopes of a Return on Investment (ROI) through efficiency gains. Most CSPs have seen the future of network digitalization and have taken the latter route. However, CSPs have been beset with high costs for data centers to maintain their cloud infrastructure. Moreover, few CSPs are maximizing their efficiency gains because their networks retain traditional, fixed, and rigid architectures within the cloud, rather than being transitioned into a flexible cloud-native architecture. In this common scenario, CSPs are unable to unlock key cloud-native functionalities like auto-scaling, GitOps, and automated lifecycle management. Fundamentally, CSPs experience increasing costs for core network resources that are under-utilized.

SaaS models present an opportunity to break free from the cost burdens of maintaining in-house legacy infrastructure. CSPs look to SaaS with anticipated benefits for cost savings, and in the survey, this was identified as a "very important" SaaS benefit. Although this was the most important priority for SaaS, faster time to value and reduced complexity were the second and third important drivers, respectively.

Figure 8: Survey Response—What Are the Key Benefits You See in Adopting SaaS Models for Core Networks? (1=Not important, 5=Very important; n=44)
Source: ABI Research



While CSPs are optimistic about the cost benefits of SaaS, they will require convincing through clear fee structures and careful Total Cost of Ownership (TCO) estimates. This is due, in part, to CSP experience with Infrastructure-as-a-Service (IaaS). Although they are distinct commercial models, SaaS typically includes some form of IaaS insofar as SaaS providers are using their own infrastructure to service software delivery. The common CSP experience of increasing OPEX under public cloud IaaS has led many to be skeptical, or at least highly critical, of cost-benefit claims. SaaS providers will need to differentiate from existing software delivery and infrastructure service approaches to communicate cost-savings.

One method of achieving differentiation is to emphasize the support that SaaS provides for the transition to cloud-native, which CSPs have struggled to achieve on their own. SaaS providers' control over both the core network applications and the underlying infrastructure presents a great opportunity to break the rigid deployments that CSPs have traditionally made in cloud environments and align with cloud-native principles. Among many other benefits, this may help validate cost-saving claims and distinguish from CSPs' previous public cloud deployments. In the SaaS model where the core network is optimized to the infrastructure by default, CSPs are free to focus more on upskilling to meet new operational demands of cloud-native orchestration and automation. Overall, the SaaS model conserves costs, while freeing investments to shift toward the most strategically important areas of network operations.

In this section, we have focused on the impact of security and cost on whether CSPs will adopt SaaS, comparing the SaaS model to standard scenarios where software is self-managed. Another essential issue to address is, once CSPs have decided to adopt SaaS, what will be their strategy for implementing it? In this case, we compare different SaaS offerings—for security, network analytics, and core network elements—to assess optimal adoption pathways. Security and cost-savings will continue to be key considerations because they will structure the risks taken along these pathways of SaaS adoption. These issues are taken up in the next section.

ALIGNING SOFTWARE DELIVERY WITH CSP SAAS ADOPTION STRATEGIES

CSPs will follow a typical deployment strategy starting from low-risk, high-ROI areas. In the context of telco software, OSS/BSS applications are a natural starting point because: 1) they are often already cloud-deployed, and even public-cloud deployed, so adoption of SaaS does not introduce significant additional risk, and 2) OSS/BSS applications directly impact network performance and telco service monetization, so they bear a straightforward relation to ROI. In the survey, CSPs identify network analytics and business applications as the best applications for an introduction to SaaS.

CSPs would also consider moving network security elements to a SaaS model first. While this has the risks of data privacy concerns discussed above, security applications as SaaS are identified as having potential benefits for speeding up deployment and detection processes (a critical factor for adopting Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR)); SaaS-based security is also identified by 84% of respondents as important or very important for Mobile Virtual Network Operator (MVNO) and enterprise expansion. CSPs wanting to target these use cases may prioritize network security applications through SaaS.

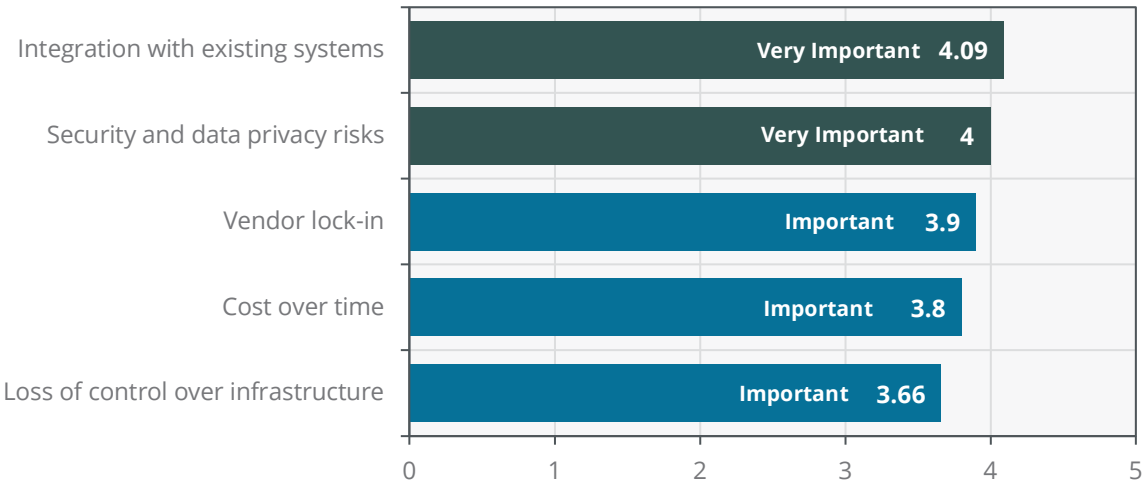
Both network security and OSS/BSS applications are easier to deliver in a SaaS model than the network core. In addition to security, there are two primary concerns here. First, for SaaS models to be commercially viable, there must be a distinction between the core network applications being delivered from CSPs' own applications, so there is a separation of these network components. As a result of this

separation, CSPs anticipate less freedom to deploy their own applications in the cloud alongside their core. Such factors create a concern among CSPs that they will encounter severe difficulties integrating their SaaS core network with existing systems.

The flip side of this is that SaaS providers would be perceived as having relatively more control over what can be deployed alongside or integrated with their own applications. So, a second closely related concern is that vendors will exert pressure on CSPs to integrate their own products with their network core, resulting in vendor lock-in.

Figure 9: Survey Response—What Concerns Do You Have About Adopting SaaS for Core Networks? (n=44)

Source: ABI Research



CSPs speak from some experience when they raise these integration concerns: 61% of respondents have already adopted SaaS for some core network elements, and only one respondent claimed to be unfamiliar with SaaS models for the core. At the same time, it is unlikely that CSPs have deployed SaaS for core network elements at scale. This may make a difference for integration.

To address these concerns, SaaS providers may clarify how broad-scale core services may differ from a highly selective use of SaaS for core elements. More generally, providers may clarify how separation of SaaS and telco applications is achieved, while still promoting integration across the stack, and their stance on the integration of common third-party applications.

Overall, the smoothest transition toward SaaS models appears to be from OSS/BSS applications and network security elements toward the core network. Of course, these decisions about "what SaaS to adopt when" are not made in theoretical abstraction from the market, but will result from practical considerations about market offerings, especially those from trusted vendor partners. SaaS providers will benefit from a broad portfolio of SaaS offerings that can accommodate different software demands and CSP profiles for risk tolerance. In the following section, Nokia SaaS offerings are considered with special attention to strategies for effectively communicating the benefits of SaaS given the survey findings.

SAAS PREFERENCES BY COUNTRY, DECISION MAKER, AND ORGANIZATION SIZE

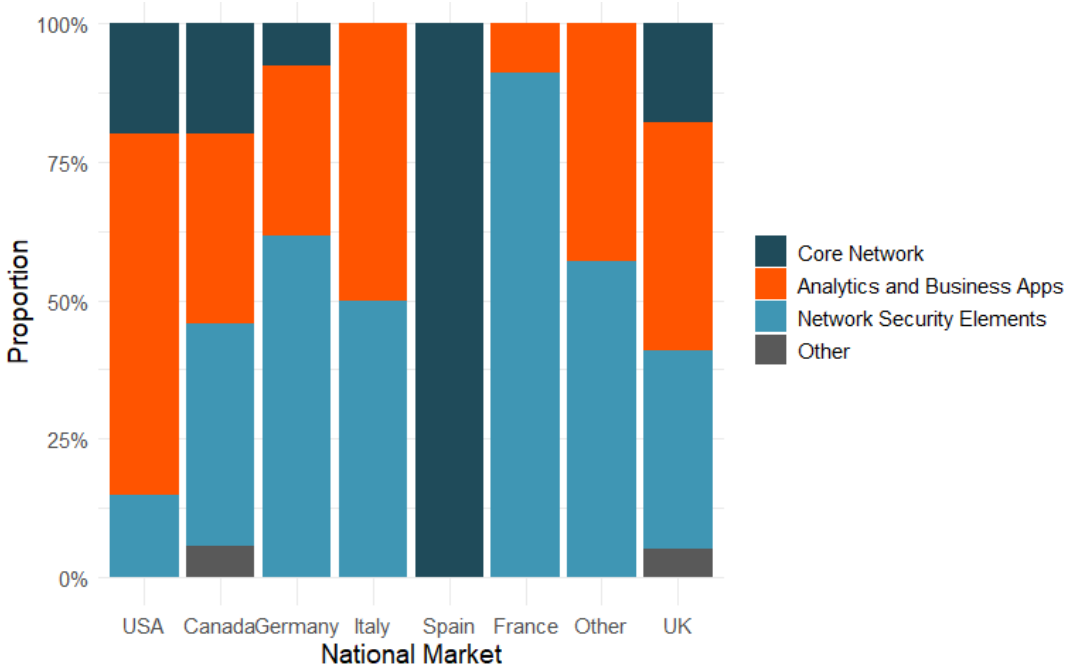
In general, SaaS priorities lean toward low-risk software like OSS/BSS applications and network security elements (Figure 4). However, there are also noteworthy differences in SaaS priorities by national market and who decides SaaS purchases within the organization.

SAAS ADOPTION BY COUNTRY

Regarding national markets, most continental European countries are risk-averse to core SaaS, so we observe greater prioritization of either network security or BSS/OSS. There are several additional factors beyond the baseline risks of experimentation with the core. First, regulatory guidelines play a major role in Europe, which include outright prohibitions on public-cloud deployment of core applications, or else strict requirements surrounding data sovereignty and security. Second, and more broadly, European countries may have regulatory processes that are less adaptive to demands of the telecoms sector, either through policy development or creating incentives for CSPs. Third, the market dynamics in each European country will play a major role in producing CSP pressure to innovate, the risk structures of innovation, and investment choices. Dynamics in European countries include competitive pressures for technologies such as telco Generative Artificial Intelligence (Gen AI), Fixed Wireless Access (FWA), or smart manufacturing; yet, compared to North American or Asia-Pacific counterparts, we do not observe high market urgency for 5G standalone adoption or cloud-native alignment outside of select markets like Turkey, Germany, and Spain.

Figure 10: Top-Priority SaaS Product by National Market

Source: ABI Research



Indeed, Spain is a significant outlier where all four respondents unanimously supported starting with core SaaS. Spain is among the most competitive European markets for 5G standalone; additionally, sovereign cloud investments between Amazon Web Services (AWS) and Microsoft Azure are nearing US$20 billion. Among Spanish CSP respondents, most cite complexity and costs of operations as key concerns, and they anticipate that future deployments will include a mix of in-house and SaaS network management. In Germany, high competitive pressures for 5G SA are counterbalanced by strict regulatory frameworks, though CSPs are closely following Telefónica's core deployment on AWS to continuously assess opportunities.

Anglophone countries reveal a more balanced distribution of CSP preferences across core, analytics, and network security elements. The United States, Canada, and the United Kingdom all have similar preferences for the core with around 19% to 23% of respondents prioritizing it. The key difference among these profiles is that the United States strongly prefers leading with OSS/BSS applications (54% of respondents), while Canada and the United Kingdom are split between OSS/BSS and network security elements.

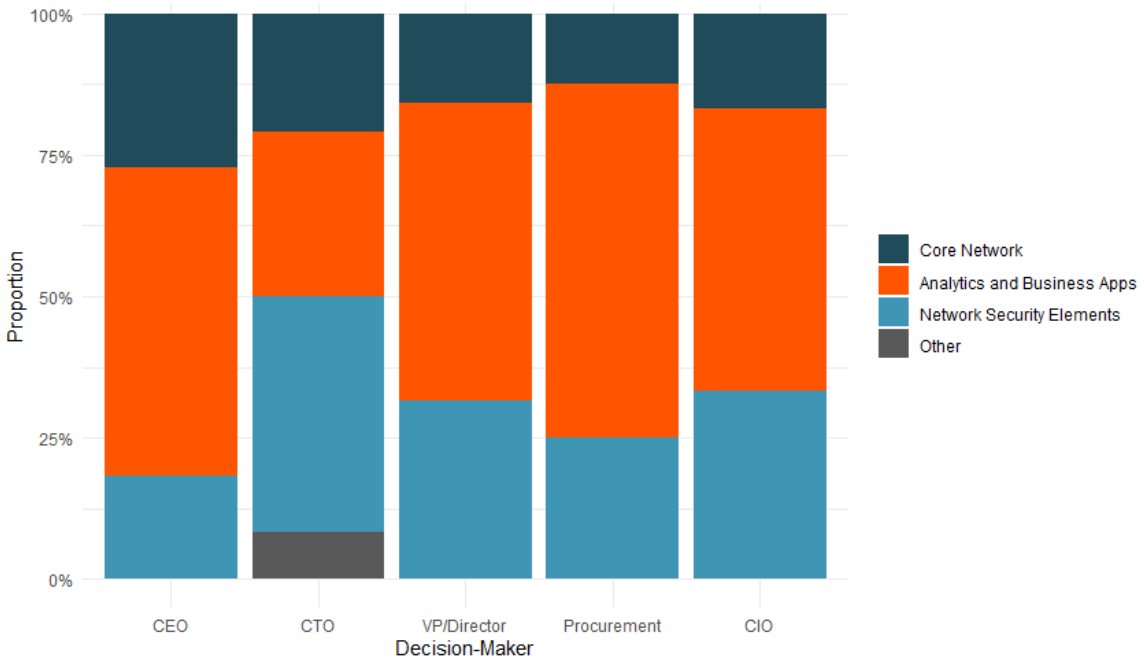
SAAS ADOPTION BY DECISION MAKER

Organizational decision makers also influence the priorities for which SaaS solutions are adopted first. To be clear, this is not in reference to the survey respondent position, but to the designation of the decision maker for SaaS purchases within the overall organization.

As with national markets, preference for core SaaS provides the clearest trends for understanding these associations. In general, the more a SaaS decision maker is separated from operations, the more likely they are to prioritize core SaaS. Or, by an alternative framing: the more attuned SaaS decision makers are to high-level business decisions, the more likely they are to prioritize core SaaS. Thus, Chief Executive Officers (CEOs) are more likely to prioritize it than Chief Technology Officers (CTOs), who are more likely to prioritize it than Vice Presidents (VPs) and directors, who are more likely to prioritize it than procurement managers.

Figure 11: Top-Priority SaaS Product by Organizational Decision Maker

Source: ABI Research



There are several factors at play here. The top challenge for adopting core SaaS is integrating with existing network infrastructure (Figure 9). SaaS decision makers who are in the direct line of these challenges may be more likely to sidestep them. Alternatively, core SaaS offers clearer risk and cost structures than self-deployed cores, and that clarity better accommodates the business decisions of C-suite executives.

Preferences between OSS/BSS and network security by organizational role are less patterned, but one line of interpretation may be offered. Where SaaS decisions are led by CEOs and procurement managers, there is a strong preference for analytics and business applications. These decision makers prioritize cost-saving efficiency and network monetization in alignment with business goals—be they high-level business goals of the CEO or product-specific ROI objectives in the case of procurement managers. Thus, sales teams should consider leading with SaaS for analytics and business applications in these contexts.

By contrast, CTOs are focused on performance optimizations through network design and configuration. Analytics applications are also significant here to ensure network performance; however, CTOs tend to value tightly integrated solutions and may prefer that it remains on shared infrastructure with existing network assets, supporting reduced latency and improving stack interoperability. Such factors may be shaping CTO distaste for OSS/BSS applications, but these patterns are not strong enough to suggest leading with network security. Rather, sales teams can add appeal to analytics applications for CTO-guided organizations by playing into CTOs' top features for analytics software: 1) AI- and Gen AI-based analytics and 2) software security measures.

Overall, differences among decision makers are less pronounced than differences in national markets, but there are still noteworthy patterns within the sample that can be used to guide sales strategy.

SAAS ADOPTION BY ORGANIZATION SIZE

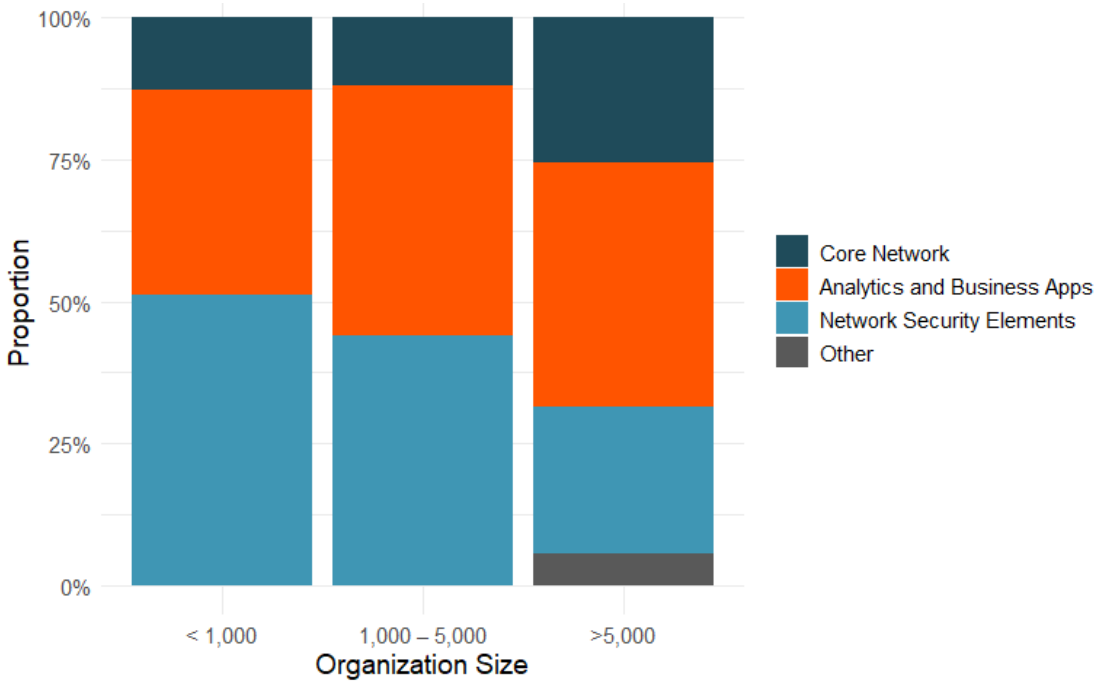
Organization size is loosely coupled with SaaS product choice. We observe that smaller organizations are more likely to purchase network security SaaS first, whereas large organizations are more likely to purchase analytics and business applications first. Here, organizational size is merely a proxy for network scale, which is the more substantive factor involved in SaaS decision-making. The complexity of a larger network may lead the mobile operator to explore outsourcing, whereas smaller organizations may prioritize simpler, targeted solutions.

Large organizations have a broader scale of network assets and bigger burden for upgrading—they may be more likely to outsource some of these challenges through a SaaS delivery model for part of the network. This would also mitigate some risks associated with SaaS experimentation, because a large portion of the network could remain self-integrated. Additionally, large organizations often have dedicated teams managing operations, enabling them to evaluate and deploy SaaS solutions in tougher scenarios. This explains why larger organizations may have a higher tolerance for core network and network analytics SaaS, on average, than smaller organizations.

Small organizations will have less network scale to experiment with and risks will be relatively higher for network applications—both core and analytics. Because their teams are smaller, they may lack the internal expertise required to customize and maintain complex network functions. By contrast, network security elements may have extra appeal for small organizations without major business units dedicated to staying on top of security protocols and continuously updating software and infrastructure. Security SaaS can address an immediate need as a first step with SaaS before considering broader adoption of SaaS for network transformation.

Figure 12: Top-Priority SaaS Product by Organization Size

Source: ABI Research

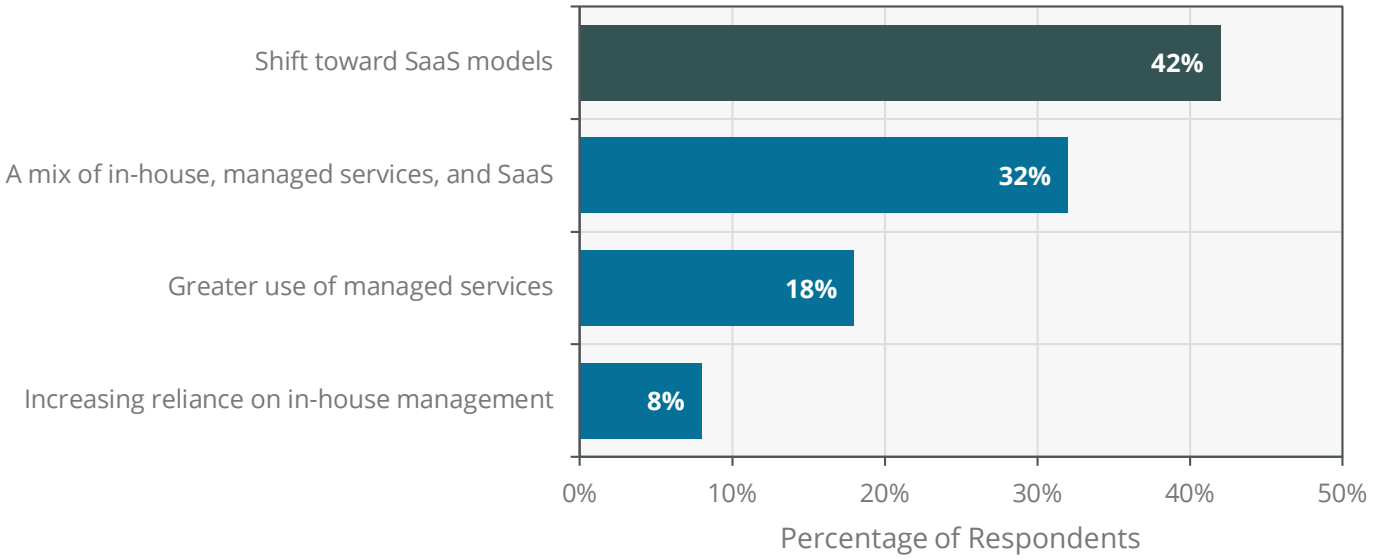


CONCLUSION: THE FUTURE OF SAAS

Our survey indicates that Mobile Network Operators (MNOs) are indeed planning to shift to SaaS business models, with some already having made the transition. However, more market education needs to take place to disseminate the benefits of SaaS and dispel several myths that surround Everything-as-a-Service (XaaS) deployment models, some of which are caused by hyperscalers. Several ABI Research contacts indicate that XaaS hyperscaler services are governed by obscure subscription and pricing models, and are sometimes dominated by ingress/egress fees. This is something that Nokia must address and ensure its SaaS pricing models are crystal clear, with assurances that future prices will remain visible today. Figure 13 validates that the largest share of respondents aims to shift to more flexible deployment models in the future.

Figure 13: How Do You See the Future of Network Management Evolving in Your Organization? (n=103)

Source: ABI Research



ABI Research expects SaaS deployment models to become mainstream in the next few years as computing infrastructure continues to become commoditized and distributed throughout the world. Nokia should accelerate its efforts to educate the market, particularly Tier One multinational network operators that are seeking more flexible business models.

Published April 2025
157 Columbus Avenue
New York, NY 10023
Tel: +1 516-624-2500
www.abiresearch.com

We Empower Technology Innovation and Strategic Implementation.

ABI Research is uniquely positioned at the intersection of end-market companies and technology solution providers, serving as the bridge that seamlessly connects these two segments by driving successful technology implementations and delivering strategies that are proven to attract and retain customers.