TELECOM TV
SURVEY 2016

WHAT DOES OPENNESS 'REALLY' MEAN?

A TelecomTV online survey in association with Wind River

in association with

OPNFV | WIND RIVER

32% ARE CURRENTLY DEPLOYING AN NFV SOLUTION

NFV INTEROPERABILITY WITH OTHER VENDORS DEEMED MOST IMPORTANT

‘OPEN SOURCE & LICENSED FROM AN EXISTING OPEN SOURCE PROJECT WITH VENDOR SUPPORT’

3.4 OUT OF 5 IN IMPORTANCE.
NO VENDOR INVOLVEMENT 2.5 OUT OF 5.

63% **DON’T EXPECT** TO GET ALL THE **RELIABILITY** AND **AVAILABILITY** THEY NEED FROM **PURE OPEN SOURCE**

Over 50% THINK DEPLOYABLE OPEN SOURCE NFV IS MORE THAN >2 YEARS AWAY

TELECOM TV

What does openness 'really' mean?

The short answer is 'many things to many people'. 'Openness' - the word - is at once positive and vague. In IT in general and SDN/NFV in particular, openness is widely agreed to be 'a good thing'. It's when you get down to the nitty gritty - especially as a user or customer - when things become problematic. How does software vendor (or Communications Service Provider) A's 'open' differ from B's? What questions do you need to ask to work out what approach is being taken? How can you make sense of the marketing material (often vague and peppered with superlatives)?

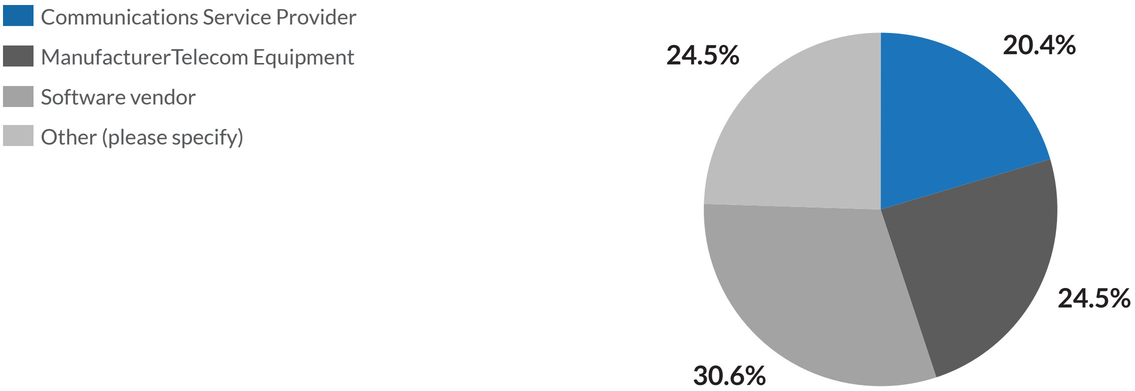
TelecomTV teamed up with Wind River to see if we could answer the openness question through a survey. We knew we wouldn't end up with a definitive answer, but we figured we could tease out the specific types of openness to see which were considered the most important by our readers and viewers.

Of particular interest for the vendor industry is the likely place of pure open source. How many CSPs looked forward to downloading open source components and using them 'as is'? How many envisaged the ongoing involvement of vendors in a new virtualized and open source world? How many viewed open source software as primarily providing a reference model against which products and specific interfaces could be built? And more...

Just as a warm-up have a look at our video - What does open really mean? - to get a feel for the variety of definitions on offer.

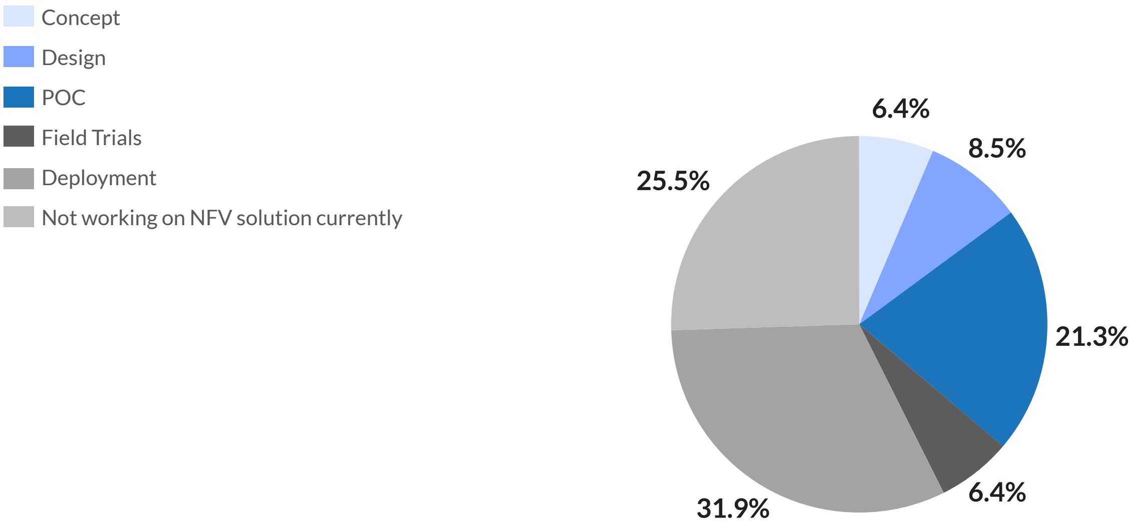
Q1. I am a...

The majority of our respondents were on the vendor side, in either software or equipment. We have teased out the differences in emphasis between vendors and CSPs for several of the key questions below.



Q2. If you are currently working on an NFV solution - as a software/hardware vendor or a service provider - what stage is it at?

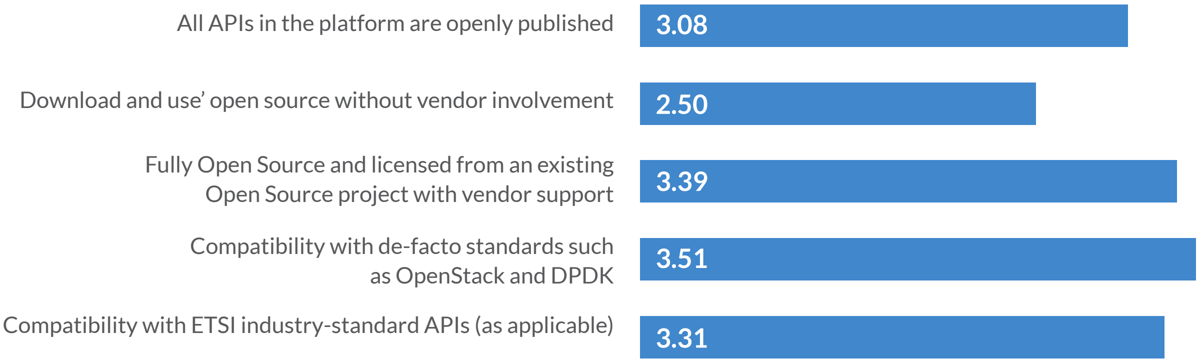
Nearly a third of our respondents claim they're at deployment stage, the majority being software and equipment vendors of course, so likely to have at least one customer/partner already



Q3. What defines an "Open Solution" for NFV?

(Please rank in terms of importance for the following elements, where 1 is the least important, 5 is the most important)

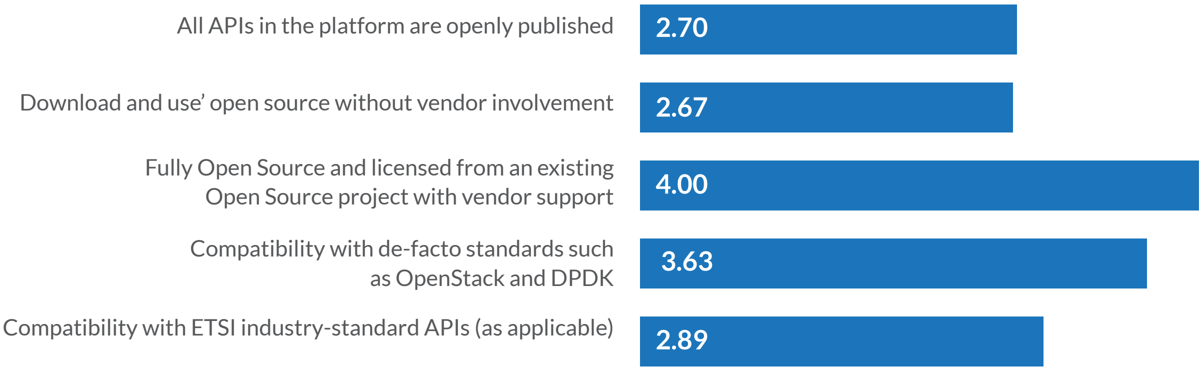
Compatibility with standards - both ETSI API standards and 'de facto' standards such as Openstack was predictably deemed most important by about a quarter of respondents. Interestingly an equal number gave ETSI a 'so-so' 3. Significant minorities assigned a 1 to both ETSI and de-facto which is interesting.
Open source with vendor involvement got a big thumbs up in aggregate while going it alone and using the components without hand-holding got a distinct thumbs down - perhaps predictably, since the survey has a lot of vendor respondents. What then is the difference between the CSPs and the full industry?



Q3. (CSPs only) What defines an "Open Solution" for NFV?

(Please rank in terms of importance for the following elements, where 1 is the least important, 5 is the most important)

The needle moved quite substantially on this question, with CSPs far more enthusiastic about both the 'download and use' and the 'open source with vendor handholding' approaches.



Q4. What other considerations do you feel are critical for an Open NFV solution?

Our respondents were given free reign with this question and ease of migration and integration featured heavily in the answers. Some CSP respondents in particular were keen to point out that they didn't just want limited interoperability, but plug and play components from different vendors in their technology estates. The underlying fear is that we'll see a creeping process of what might be called 'de facto' lock-in to particular vendors or 'ecosystems'. In other words, just enough non-compatibility to make it difficult or costly to step outside a specified ecosystem.

This unease was expressed, in my opinion, by the following mix of statements by respondents. "Demonstrated interoperability in live networks"; "Future-proofed by having !00% of code upstream and supported by multiple vendors".

Some respondents were very specific and detailed: "1st priority: all interfaces from VNF to NFVI and MANO open (to avoid VNF vendor to write to each of about 10 possible environments) 2nd priority: MANO / NFVI internal interfaces open, and/or with support of well defined "plug in" adapter interfaces - to allow interchange of the infrastructure components".

Another contribution offered: "First target must be VNF-NFVI 'AND' VNF-MANO interfaces. MANO internals etc. are less important (as they are at least contained within the infrastructure while VNF interactions affect every VNF vendor). VNF-MANO particularly is holding back interoperable solutions -- we should have a way to describe and deploy stuff by now, but there is no way (or more often vendor-specific ways). OPNFV needs to [come to the] rescue here." Also mentioned: "Tight co-ordination amongst open-sourced projects like OPNFV, ODL and OpenStack."

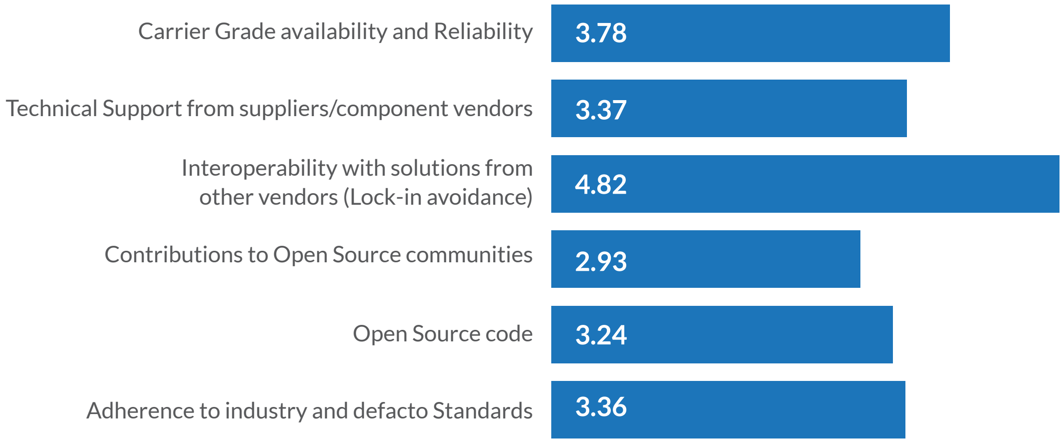
"[Solutions] should not force proprietary or quasi-open protocols, software or hardware in order to utilize the system to 100% of its feature set. [Components] should be replaceable with another vendor's products without making substantive changes to the management, provisioning or other software/hardware elements."

But there was also an understanding that full compatibility and interworking was all very well, but what was required was a fast and inexpensive way of testing the solutions: "Online interoperability testing available without prior contact or agreements," stated one hopeful respondent.

Q5. When creating a Proof of Concept or prototype...?

(Please rank in terms of importance for the following elements, where 1 is the least important, 6 is the most important)

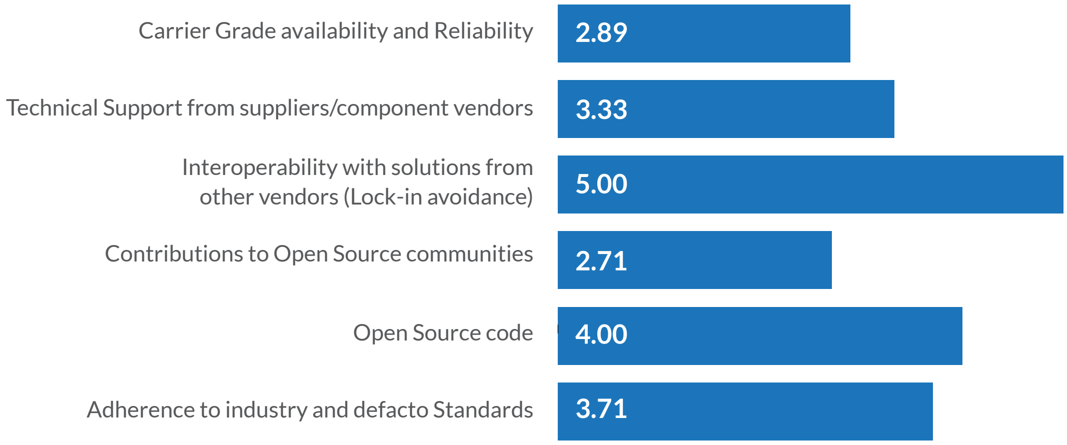
Interoperability and carrier-grade reliability were firmly favoured in the aggregate result.



Q5. (CSPs only) When creating a Proof of Concept or prototype...?

(Please rank in terms of importance for the following elements, where 1 is the least important, 6 is the most important)

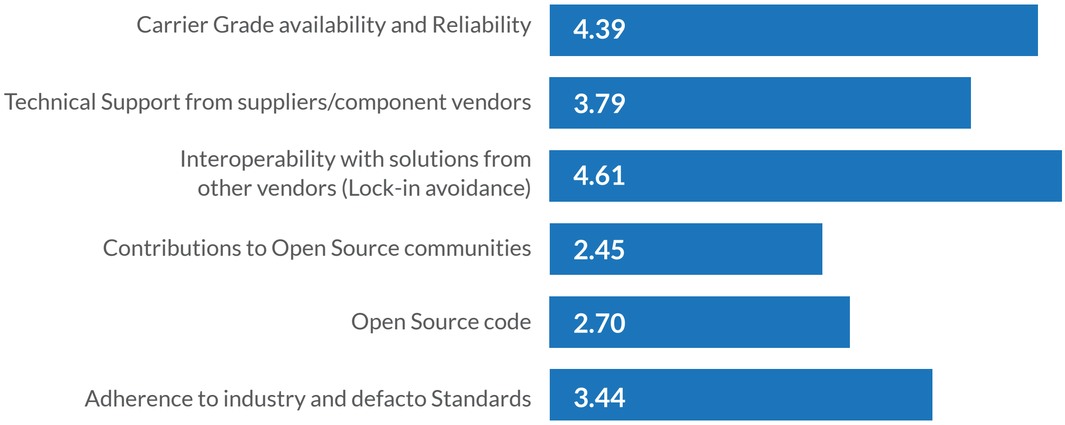
The interesting difference here is that CSPs were, in aggregate, slightly less inclined to rank carrier grade performance. Perhaps this difference might indicate that vendors are adhering to 'carrier grade' as a selling point more than CSPs are, but it's also true that CSPs might be less inclined to rank carrier grade as important at the Proof of Concept stage.



Q6. When deploying a commercial product...?

(Please rank in terms of importance for the following elements, where 1 is the least important, 6 is the most important)

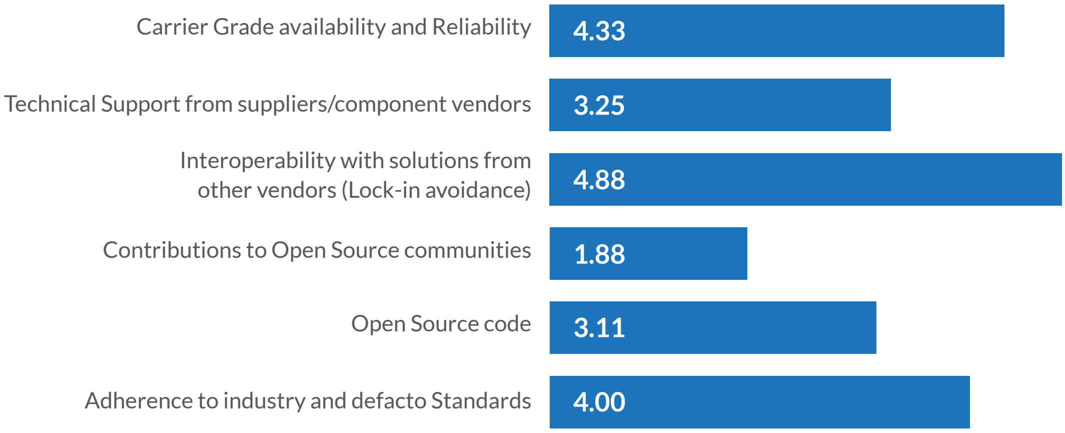
Interoperability and carrier grade availability won out again.



Q6. (CSPs only) When deploying a commercial product...?

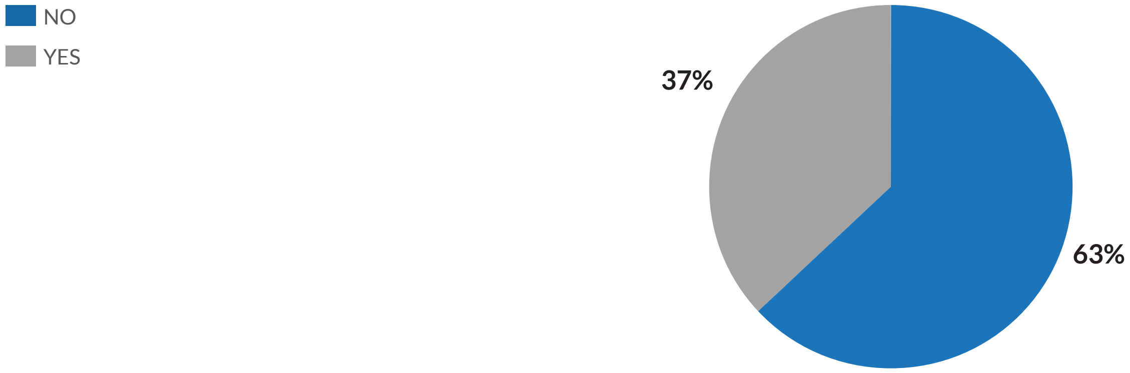
(Please rank in terms of importance for the following elements, where 1 is the least important, 6 is the most important)

Sure enough (see Q5, CSPs only) when it comes to commercial deployment CSPs assign far greater importance to carrier grade. Not surprisingly Interoperability leads in importance to CSPs with carrier grade and industry standards not far behind. Contributions to open source communities seems less important in this category.



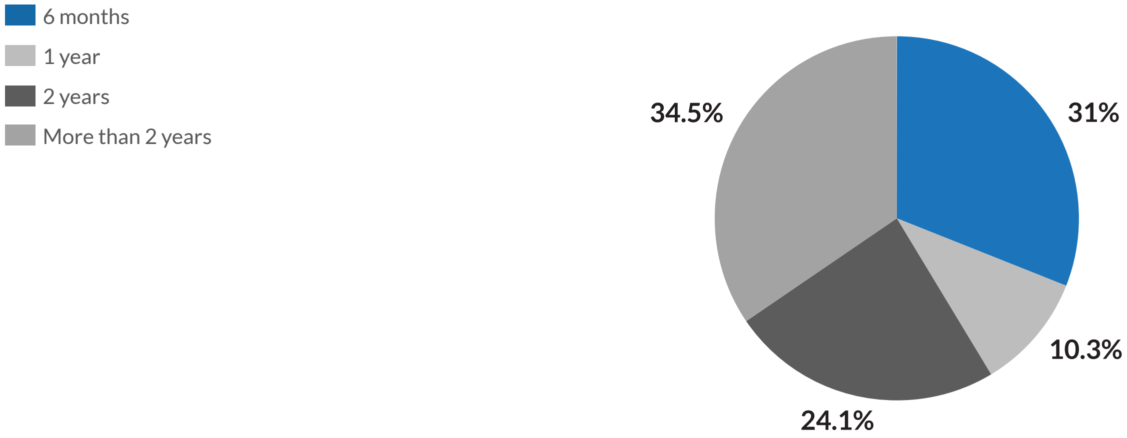
Q7. Do you expect to get all the reliability and availability you need for a commercially deployed NFV solution from pure Open Source?

A clear 'no' to this question, although over a third of respondents thought they would.



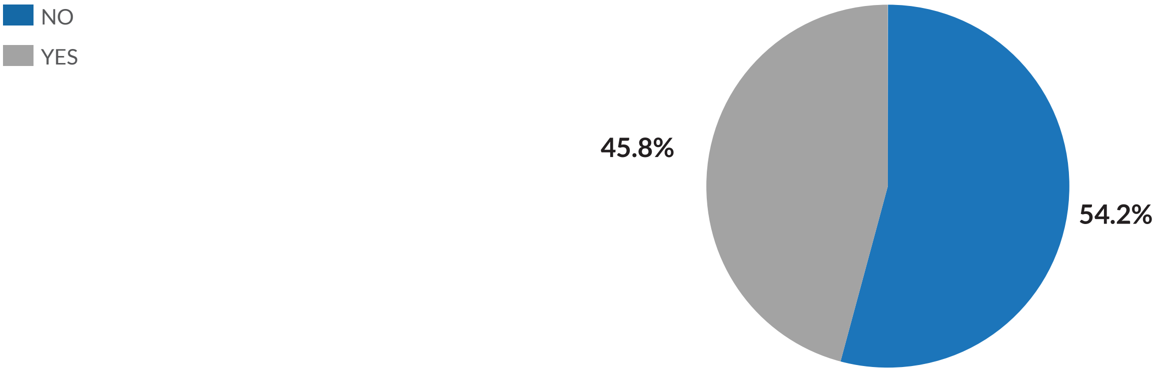
Q8. If yes, when do you anticipate having access to an open source solution that meets your deployment reliability and availability needs?

And one third of the 'yes' vote are resigned to waiting for at least another two years before an appropriate open source solution becomes available.



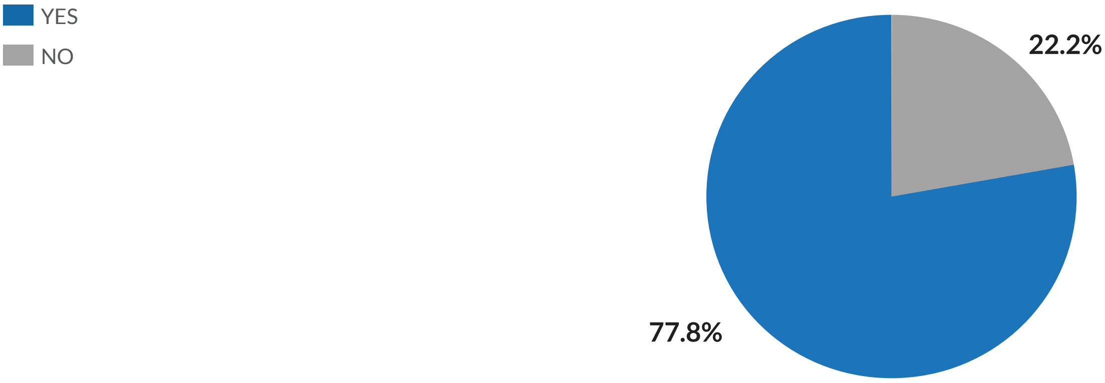
Q9. Do you expect to get the performance you need for a commercially deployed NFV solution from pure Open Source?

Here the gap narrowed somewhat with 45% saying that, performance-wise (as opposed to reliability and availability) they thought the virtual experience would be adequate with about 55% saying it wouldn't.



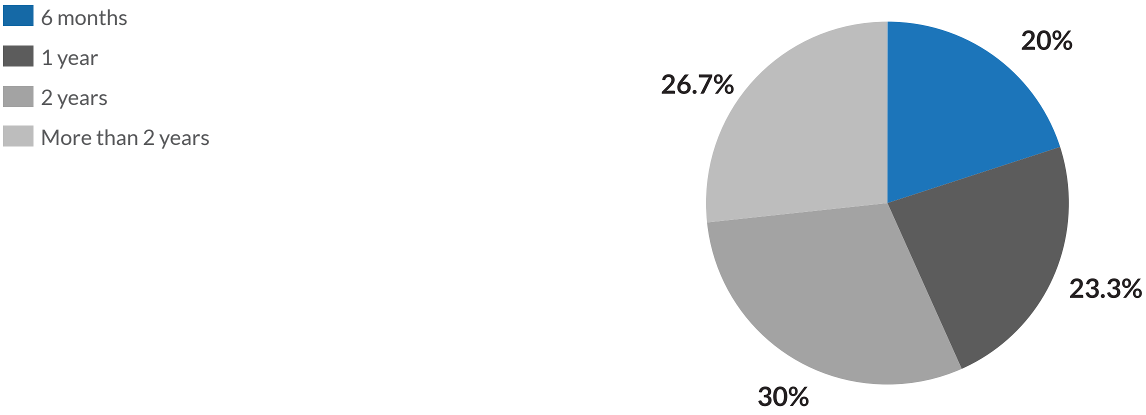
Q9. (CSPs only) Do you expect to get the performance you need for a commercially deployed NFV solution from pure Open Source?

CSPs on their own, however, were far more optimistic, with only 22% saying they thought performance wouldn't be up to the mark, with 78% saying they thought it would.



Q10. If yes, when do you anticipate having access to an open source solution that meets your deployment performance needs?

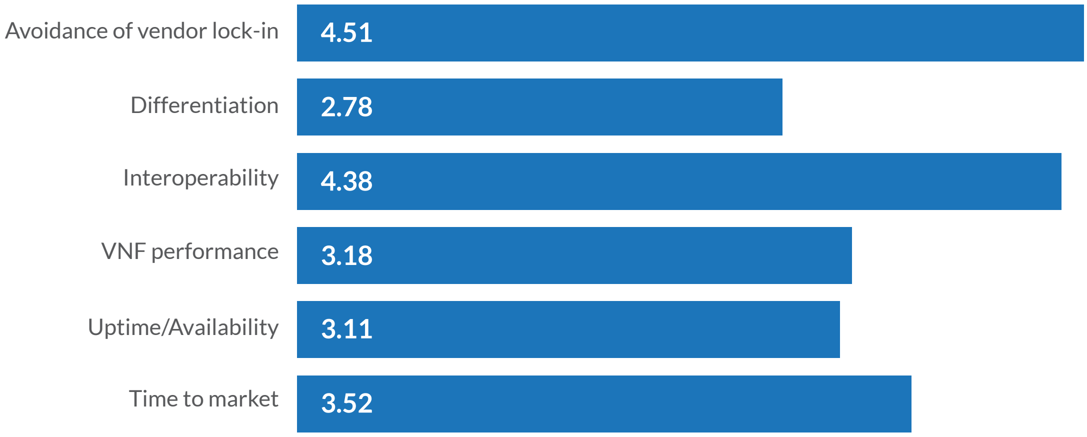
In line with the more positive performance expectation, a far higher proportion of respondents narrowed their time-scale on when that adequate performance would become available, with most opting for two years.



Q11. How important is an open solution when considering...?

(Please rank in terms of importance for the following elements, where 1 is the least important, 6 is the most important)

Interoperability and lock-in avoidance are the overwhelming concerns.



Q12. Are there any other considerations you wish to share?

“Some of these answers aren’t as black and white [as] performance is based on traffic load/scale. Introduction of some of these on open source are fine for smaller, more focused markets.”

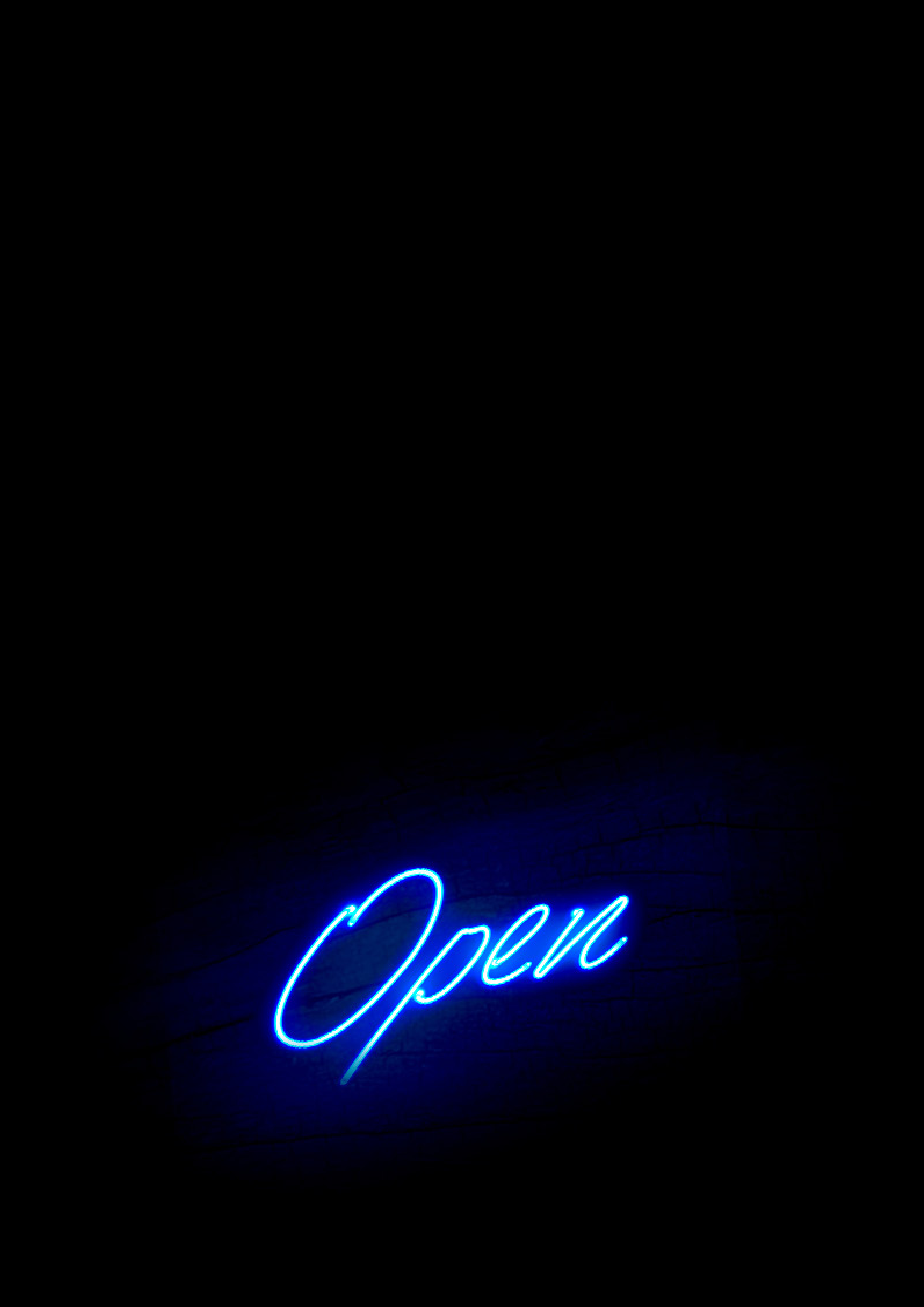
“We expect the management and orchestration layers to be open source [to] allow vendors to compete for specific VNFs with their own code and fight over performance, reliability and end-user benefits.”

“Open Source is very important but packaging of open source to meet deployment & operational needs will still be required and will be provided by vendors that deploy Open source distributions and commit SLA & Support.”

Conclusion

So what does Open mean? Clearly it means slightly different things depending who you ask and when you ask them. When we teased apart vendor answers vs CSPs it was also clear that each group placed different values on some key components.

Another interesting observation is how the importance of key components varies depending on the phase of the project. One thing that was very consistent was that vendor lock-in is something to be avoided and openness, in whatever form, (open source, open standards) plays an important role.



Open