| | |
|---|---|
| **In what capacity or on whose behalf are you participating in this public consultation?** | Cloud service provider (also includes providers of cloud infrastructure, independent software providers and intermediaries) |
| **In case of representing a company, please specify the type of company:** | Large company |
| **Full name (of the participant or represented institution):** | SAP |
| **Do you wish to make your name publicly available with your answer or keep it confidential (in which case it will be published as an anonymous answer)?** | Public |
| **Contact email (will remain confidential)** | [CONFIDENCIAL] |
| **1. In your opinion, what will be the main factors that will drive the growth of the sector in the coming years? (max. 300 words).** | |
| **2. How would you classify the different types of agents/operators involved in the cloud market value chain? (max. 300 words).** | |

| | |
|---|---|
| **3. Would you highlight any particular feature of the cloud market in Spain as compared to other European countries? How do you assess the overall competitive situation of the cloud market in Spain? Are there any particularly significant trends? (max. 300 words).** | |
| **4. In your opinion, what are the main elements that determine the dynamics of competition among cloud service providers? In your opinion, which other markets can affect the competitive dynamics in the provision of cloud services? (max. 300 words).** | |
| **5. In your opinion, when contracting cloud services from an operator, how do the main providers' offers differ from each other? (max. 300 words).** | |

| | |
|---|---|
| **6. When contracting cloud services from an operator, describe in order of importance the factors that, in your opinion, are the main determinants of the contracting decision, such as, among others, price, technical quality of the service, the provider's portfolio of services, security, transparency of the contract, nationality of the provider, previous relationship with the same provider, previous knowledge by the staff, etc. (max. 300 words).** | |
| **7. When contracting cloud services from an operator, assess the extent to which contract terms and conditions are negotiable (max. 300 words).** | |
| **8. Indicate what difficulties may arise, at the time of contracting a provider's cloud services, to anticipate the final cost of use of the contracted service (max. 300 words).** | |

| | |
|---|---|
| **9. Assess the transparency of contract terms and conditions and indicate whether changes in contract terms and conditions are common (max. 300 words).** | |
| **10. In migrating to the cloud, explain the role of the integrator or intermediary, and its relevance to the competitive dynamics of the market (max. 300 words).** | |
| **11. For software development companies offering independent cloud-based software applications, consider which are the main channels to reach the end customer and the factors on which the choice of the chosen channel(s) depends. When offering independent cloud-based software applications, consider whether it is possible to do so in more than one marketplace from a vertically integrated provider (max. 300 words).** | |
| **12. Assess the conditions required to intermediaries to be able to sell the products of one or more cloud service providers, and whether in your opinion they affect the competitiveness of the final solution offered by the intermediary in relation to other sales channels (max. 300 words).** | |

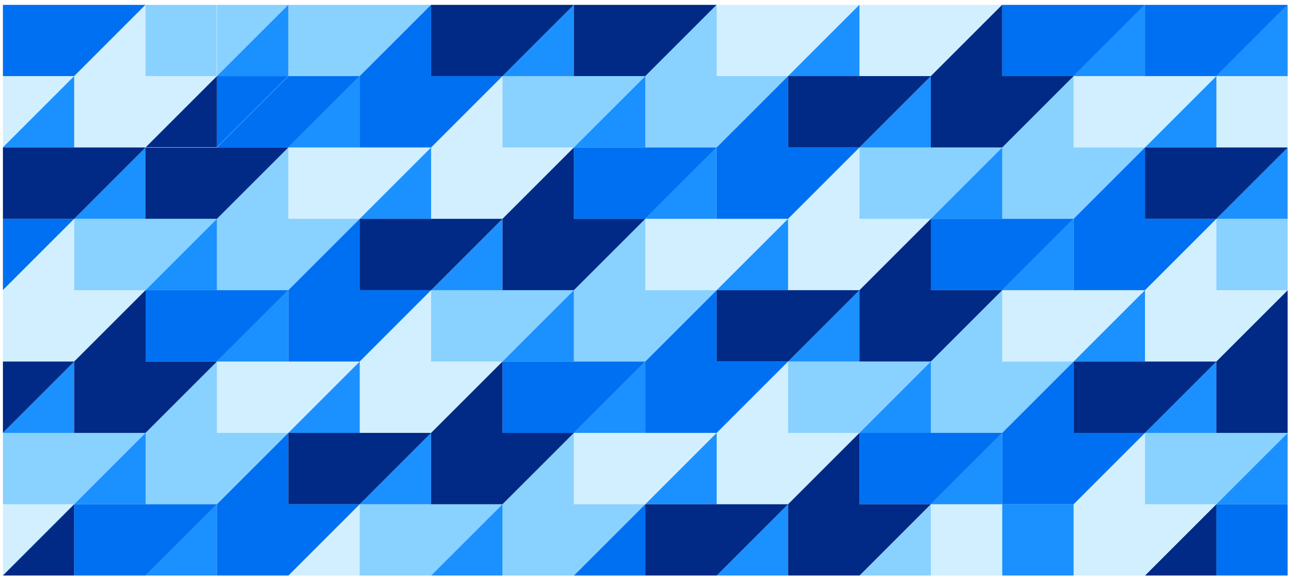
| | |
|---|---|
| **13. Assess whether there are significant barriers to entry in the cloud services or cloud infrastructure market. If so, indicate and describe what type of barriers (e.g., regulatory, investment size, availability of qualified staff, other) and indicate which services or cloud layer (IaaS, PaaS, SaaS) are affected by each barrier (max. 300 words).** | |
| **14. In your opinion, assess which cloud layers (IaaS, PaaS, SaaS) present the greatest competitive challenges and explain why (max. 300 words).** | |
| **15. For companies already present in the cloud market, what are the main obstacles to their activity and to competition in the sector? (max. 300 words).** | |

| | |
|---|---|
| **16. Assess what technical or economic difficulties exist for migrating to the cloud. Indicate, in your opinion, which solutions could be implemented to mitigate them (max. 300 words).** | Cloud migrations difficulties have been deeply identified and discussed during the Data Act legislative process. EU harmonised enforcement should be a priority at national level avoiding any additional complexities to what has been approved in the Data Act. See attached (sent to dp.estudios@cnmc.es) SAP detailed implementation point of view on switching provisions. |
| **17. In your opinion, once the services of one cloud provider have been contracted, what technical, economic or other factors might make it difficult to change provider? In your opinion, which solutions might be implemented to mitigate these difficulties? (max. 300 words).** | |
| **18. In your opinion, what are the difficulties in contracting the services of more than one cloud provider? In your answer, please assess aspects of vertical interoperability (between services located in different cloud layers), horizontal interoperability (between services located in the same cloud layer) and interoperability of the data produced when using different cloud services. In your opinion, what solutions could be implemented? (max. 300 words).** | Cloud interoperability difficulties have been deeply identified and discussed during the Data Act legislative process. EU harmonised enforcement should be a priority at national level avoiding any additional complexities to what has been approved in the Data Act. See attached (sent to dp.estudios@cnmc.es) SAP detailed implementation point of view on interoperability provisions. |

| | |
|---|---|
| **19. Assess the advantages and disadvantages of adopting interoperability standards or protocols, including their impact on competition and/or innovation (max. 300 words).** | |
| **20. When contracting services from the same cloud provider, and from the point of view of its commercial offer, assess what obstacles exist to contracting each service separately (max. 300 words).** | |
| **21. When contracting additional services from a cloud provider, assess the relationship between contracting these services and the discounts for the use of additional services (max. 300 words).** | |
| **22. Assess the existing obstacles to competition in the public procurement of cloud services, and indicate the solutions that could be implemented in your opinion (max. 300 words).** | |

| | |
|---|---|
| **23. Provide additional comments on other barriers, distorting factors or issues that you consider relevant to the functioning of this sector (max. 500 words).** | |
| **24. Assess the current European and national regulatory framework in its ability to promote an efficient and competitive operation of the cloud services market. If so, how could it be improved? (max. 500 words).** | |
| **25. In your opinion, what other regulations could affect the competitive dynamics of the cloud sector? If so, how could they be improved? (max. 500 words).** | |

| | |
|---|---|
| **26. Provide additional comments on other solutions or recommendations (not necessarily of regulatory nature) to improve the competitive dynamics in the cloud sector (max. 500 words).** | |



# SAP Point of View

# The Data Act

# Standards and specifications for Interoperability and Switching

# Table of contents

This paper covers the SAP point of view on the implementation issues arising from the Data act Chapters 6 and 8 with a particular focus on the new standardisation powers found in Articles 30, 33, 34 and 35.

## Section 1: Regulatory overview and general recommendations

Although the Data Act uses a close similarity with the New Legislative Framework in Article 33 with the addition of a limited power to use alternate common specifications to harmonised standards, the Data Act deviates from the 'New Legislative Framework' (NLF) in a number of significant ways in Articles 30, 34 and 35. This paper first looks at the implications of this for the Commission and Member States delegates to the Article 46 committee.

The NLF approach sets out mandatory 'Essential Requirements' that are backed up by voluntary standards (or solely in the case of Article 33 of the Data Act a voluntary common specification). These are specific standards granted 'harmonised' status meaning compliance gives a 'presumption of compliance' with the Essential Requirements. This allows the 'safety valve' of a company to diverge from the standard and appeal directly to the legal text of the essential requirements if the harmonised standard suffers scope creep or is not technology or business model neutral.

By contrast the Data Act has no essential requirements in Articles 30 and 34 and the status of the essential requirements in Article 35 is unspecified. It therefore seems a reasonable interpretation that at least any standard that is 'harmonised' or becomes a common specification under Articles 30 and 34 (and possibly Article 35) effectively becomes direct technical regulation and compliance is required for market access.

Ambiguity and scope creep are therefore significant risks as there is, per se, no limit on scope in the absence of essential requirements in Articles 30 and 34. A key principle of standards is that they have the maximum impact and the minimal adverse effect on innovation when they are limited to the smallest possible scope required to have their desired effect. Where the desired effect is poorly defined, achieving this becomes a significant issue. As such, in the preparation of a request for standardisation or consideration of an open specification, it is vital to both consult effectively and remove ambiguities of the intended effect and limit the scope as this is in effect a new approach to market regulation.

**Recommendation 1: The Commission should undertake full public consultation whenever it proposes a 'request for standardisation' relevant to Data Act implementation.**

In the context of cloud, we have a relatively small number of implementors and a large user base. It is therefore vital that consensus does not become users versus implementors as what is in effect a regulation that is too costly, or in the worst case impossible to comply with, simply drives customers and suppliers away from the cloud delivery model. We must further avoid niche or specialist requirements unfairly adding unnecessarily to the overall cost base.

**Recommendation 2: The Commission should undertake full public consultation on the final step of granting the output of a request for standardisation harmonised status, recognising that in the case of at least Article 30 and 34 this is effectively a direct regulation of the market as opposed to a voluntary 'presumption of conformity'. Any such act should be compliant with WTO TBT Annex 3 recommendations including the consultation requirements.**

In allowing the use of as yet unidentified 3rd party specifications as common specification that could be as binding as a regulation, a number of new issues arise. Any specification that becomes a Data Act 'Common Specification' under Articles 30 and 34 becomes a direct technical regulatory requirement (and possibly Article 35). The formal Member states' standards bodies and the European Standards Bodies CEN/CENELEC and ETSI have well defined processes and are compliant with the requirements of international trade agreements.

They also have strict and clear drafting guidelines that have stood the test of time in clearly communicating objective requirements.

Similarly, they have proven IPR policies for contributors and commentators, robust decision processes and transparency arrangements. In particular it is an absolute requirement that any technical information that would need to be incorporated into product e.g. data structures, formats, code extracts and similar must be of completely known provenance and licensed in a way that is compatible with all open source and proprietary software developments (e.g. permissive open source licensing).

Whilst there are many established bodies with an equal claim to well-formed processes and compliance, some new or recent ad hoc bodies would create a significant risk and require greater scrutiny. Whilst there is a limited recognition of this by reference to Annex II to Regulation (EU) No 1025/2012 in Article 35 it is not present in Articles 30, 33 and 34. Annex II to Regulation (EU) No 1025/2012 requires key elements of these to be in place but does not provide criteria to assess those requirements.

**Recommendation 3: The Commission should undertake full public consultation on any open specifications being considered as candidates for common specifications, whilst considering WTO TBT Annex 3 recommendations including the consultation requirements, as these are in effect potentially creating direct regulations. Such consultations must include a review of the policies and practices of the originating body with particular regard to stakeholder engagement, consultation, decision making, maintenance and IPR policies. Full documentation must be available on the provenance of any technical content, and it must be licensed in a way compatible with all software development business models.**

There is a further area of consideration in that for the first time NLF style arrangement and use of standards for regulation outside of the normal political process are being applied to services that are intended to be changed and updated during the time of deployment. Although in most cases this should have limited impact for use of mature technical or process standards, less mature standards or new approaches, especially anything with security implication or that contain 3rd party IPR, cannot be set as mandatory without allowance for changes in response to emergent security threats or infringement risks.

**Recommendation 4: Implementing acts granting either harmonised status or common specifications should allow for exemptions, either time limited or until the standard or specification can be updated whichever is longer, in the event of third party IPR claims or security issues emerging**.

**Recommendation 5: The Commission should include in the above recommended consultations the approach to compliance intended with a basically static standard applied to a dynamic service including such aspect as notification of divergence, frequency of compliance check and similar issues.**

## Section 2: Market overview

Broadly speaking the cloud market is separated out into the well know Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

Breaking this down we can broadly look at the IaaS layer as described in article 30(1), IaaS providers compete with traditional servers and infrastructure and are a highly consolidated market dominated by a few hyperscalers. It is, to a large extent, a foundational layer in that it is used by all the other layers and used by those running their own applications. IaaS includes bare metal options where customers deploy their applications directly to the server and virtualised environments, including virtual server technologies and container services. IaaS truly constitutes a market.

By contrast SaaS is a mix of independent software applications delivered either on their own infrastructure, on PaaS or on IaaS. They compete within their own SaaS subcategory (supply chain management for example) and their on-premise equivalent. In that sense there is no 'SaaS market' rather it is a cloud-based delivery model for the given software applications. Further these may be focused to increasingly specialised sectors – health record management, hospitality and so on.

Another important factor to consider about SaaS is that the SaaS vendor has full responsibility for delivering, operating, securing, and maintaining the solution for their customers. This is particularly important in the case of multi-tenant SaaS solutions where processing resources are shared between all customers, rather than dedicated per customer in a single tenant model.

Contractual agreements between the SaaS provider and the customer include clauses such as service level agreements (SLA) that the provider must meet, notably regarding availability of the solution and data security and protection. For these reasons, the SaaS vendor is wholly responsible for their development and infrastructure choices. This includes their choice of platform provider (IaaS, PaaS, own infrastructure), technologies (open-source software, commercial solutions, PaaS services) and tooling (ticketing solutions, monitoring services, security solutions). The SaaS vendor may offer configuration choices to their customer (e.g. data processing location), but by principle they have no obligation, other than commercial or compliance reasons, to deliver their services based on the preferences or requirements of each individual customer. Rather the obligation is to ensure fair treatment across the customer base and for market competition to deliver to significantly varying requirements.

Although the term multi cloud may be widely used it should be distinguished between IaaS where it is used to describe use of services that should be largely competitive and substitutable and SaaS where it could simply refer to using multiple SaaS applications via one or more SaaS vendors and those applications are running on one or more delivery models or vendors.

It is also worth distinguishing that, a IaaS or PaaS customer will hold a license to the code or application running on the IaaS or PaaS infrastructure and it is logical for a commercial application or custom code running on IaaS or PaaS model to be portable to another vendor's environment, providing it has been developed in a vendor agnostic way or where there is a competitive supply of compatible IaaS or PaaS solutions

In the SaaS model, the customer has a usage license, with ownership of the data processed in the solution and higher order user defined data structures where supported. The customer will also have been responsible for the integration between interoperable services in a way that reflects their unique solution set and individual business processes. The format of the data within each application is normally unique and may be proprietary to the SaaS application. This distinction is important when considering switching since it is not logical to expect the data of a SaaS application to be portable from one vendor's application to another without transformation. This transformation process is the responsibility of the data owner especially considering the need to sustain any required integrations with other services.

This is largely a more detailed distinction that that defined in article 2 'the same service type' defined as "Data Processing Services that share the same primary objective, the same model and the same functionalities" logically noting that means the sector-based customer as part of the primary objective.

PaaS has been mentioned above as a possible delivery platform for SaaS solutions.  These can vary from services specifically tied to an underlying IaaS (often termed 'serverless' as the IaaS provider automatically handles the provisioning on their system) or can be a suite of applications and services that support multiple IaaS or on-premise systems.  In the latter case, the PaaS consumer is presented with access to a set of applications and services that may be commercial offerings, open-source software and vendor specific services. The consumer decides which applications and services to use when building their solution.

In this scenario a PaaS vendor develops and proposes specific services that may not have a direct equivalent on another PaaS vendors platform. This could include object and data storage solutions, security tools such as encryption management tools, data analytics solutions and artificial intelligence technologies. The vendor may also use bespoke hardware to run their applications.

If a consumer chooses to develop their solution using vendor specific applications and services, they will need to redevelop their solution to run on an alternative PaaS platform if they wish to switch vendors. The consumers' decision to tie themselves to a specific PaaS platform, just like their usage of a SaaS solution, must be considered a consumer's choice and not be subject to portability and interoperability requirements.

It is also necessary to avoid simplistic approaches to complex market facing definitions.  Boundaries can blur and the level of support for user defined code artefacts – scripts, macros and similar are present in many services.

These categories and differences need to be reflected in any approach.

**Recommendation 6:  Interventions through the standards process should differentiate their scope clearly between IaaS and SaaS and handle and distinguish PaaS depending on the level to which it is tied to a IaaS provider.**

## Section 3: Recommendations on implementation for SaaS

Although some attempt at distinction is made in the text of the Data Act between interoperability and switching, the cross referencing between Chapters 6 and 8 in Articles 30, 34 and 35 and therefore between interoperability and switching means that the interpretation of the Data Act itself is challenging and could lead to ambiguous and poorly targeted requests.

**Recommendation 7: When setting out the expected request(s) for standardisation we would strongly recommend that the existing standards definitions, primarily from ISO/IEC 19941:2017 as recognised in recital 90, are used and any deviations clearly documented and justified.**

Clarity is also needed in the following areas:

Intended Lifecyle segment - We would add the need to specify the focus on the intended standard during the acquisition lifecycle.  Portability as a subset of switching is primarily focused on pre-procurement qualification and at contract termination, interoperability is during 'parallel use' to quote article 34 and therefore during the contract.  As such specifying the lifecycle stage focus of any request is vital.

**Recommendation 8: Clear statements should be made in the request for standardisation as to the intended part of the consumer adoption lifecycle – pre-contractual, contractual and post contractual and clear separation between interoperability as  'parallel use' and portability as part of 'switching' between competitive services should be maintained.**

Intended targets – vendor vs customer.  A standard or specification aimed at unilateral vendor compliance is significantly limited by what is logically possible.  Compatibility in all the areas related to porting or interoperability (policy, semantics, syntax, transport mechanism, security and transfer protocols) with unspecified and unknown 3rd parties is not possible and therefore cannot be specified.  Limited success in complex environments can be specified by requiring compliance with an independent technical standard (as is in effect done with normal machine-readable data file formats or sector specific uses) but the objective is only obtained if the end user limits themselves in that way so the focus is actually on customers.  There are certainly sectors with mature standards for interoperability e.g. finance or travel.

Intended targets – generic vs sector.  A generic standard or specification is again highly limited as to what can be achieved beyond the lowest common level of technical specification as higher order semantics (data structures etc.) are sector or user defined.

In summary a generic vendor cloud standards would largely be limited to the transparency requirements already set down in Article 25 and low level, lowest common denominator specifications.  Although there is a rationale for standards to support common approaches to transparency there is limited impact on compatibility for interoperability or portability (as a precursor to switching) beyond creating common formats for transparency statements.  This can possibly ease customer due diligence in reviewing and comparing transparency statements but little other impact.  Even in that situation, experience with prior attempts suggests strongly that customers are more interested in specific questions for their own scenarios than voluminous documentation on transparency of all the various data exchange processes that could possibly be used.

As such, SAP would strongly recommend a focus on sector segmented customer groups for SaaS for each sector or market segment (HR, finance, automotive, health etc).  This is ideally where customer stakeholders are able to represent a significant market share and can be willingly brought together for standardisation.  In effect this means any area where the otherwise individual business processes that create barriers to switching and interoperability can be moved to common processes without impacting competitive advantages. Ultimately the widest possible adoption of a standard by the customers in a given sector in actual use, as opposed to a procurement criterion is the only solution to compatibility. Implementing a standard without clear customer value add or sector wide adoption would at best be a waste of rare and expensive developer resource. Any such compulsion would increase the cost of supply with no added value. It is also vital this be customer led to avoid dominant vendors forcing customers into unsuitable or biased specifications.

This sector or market segment approach for SaaS should start with a clear sector analysis looking at existing levels of common business processes, and mature sector representative bodies and standardisation within each sector or segment in order to prioritise the most tractable sectors first.

**Recommendation 9: We recommend that the request for standardisation should be customer and/or market segment led, as that represents the biggest improvement in generating a competitive market of SaaS suppliers and will ensure interventions truly represent added value for customers with the Commission developing a clear criteria led approach to sector analysis and prioritization.**

We also note that the many complexities occur in terms of supporting interoperability within the single market by varying practices across the EU Member States covering data exchanges between business and government both for transactional matters (public procurement) as well as compliance matters (tax and finance matters at both company and employee level, data retention, social payments and open data projects and regulations). These include varying approaches to XML Schemas and APIs which need to be supported by each customer in each country. This mandates not only a sector by sector but country by country approach to switching and interoperability for any business process that includes data exchange or reporting to the public sector often driving bespoke customer modifications.

Whilst the proposed Interoperable Europe Act, now entering a pilot phase, is proposing a focus on assessing interoperability for **cross border** data exchanges we note that **in country** differences between member states creates market silos due to the lack of interoperability and impact on switching or multi cloud use.

**Recommendation 10: The sector based approach should be supported by analysing each sectors B2G implications and a review of differing data exchange approaches in Member States and a commitment by Member States to engage fully in each sector's standardisation activities where a B2G issue is present.**

**Recommendation 11: As part of the overall gap analysis, Member States should analyse and compare their internal and B2G data interoperability mandates as well as cross border initiatives and identify priorities for standardisation at EU level. This recognises that Public Sector is in this sense a customer sector of its own with unnecessarily varying processes and specifications but also has a significant wider impact on other sectors interoperability and switching both transactionally and via regulation.**

# Section 4: Recommendations on implementation for IaaS

IaaS is called out separately in Article 30 although is still covered by in terms of standardisation powers in article 34 and 35.  IaaS is best viewed as a market segment in its own right as per the discussion in section 3. SAP is of course an extensive customer and in part reseller of IaaS.

Again, we would follow the logic in section 3 and suggest a broad consensus of IaaS customer requirements is the main target of the necessary standards request but noting that SaaS vendors form a significant sub-part of that customer base with a clear interest and access to the required technical expertise.

SAP would prioritise standardisation to create a clear stable and consistent abstraction layer. A clear, stable and consistent abstraction layer effectively ensures that hyperscaler/platform independent solutions could be created in a reliable and stable way to allow switching and multi cloud use.

However, although this is a clear goal, it should not be taken as preventing platform or supplier specific innovations which deliver clear customer value add and allows hyperscalers to differentiate themselves.  The aim is to ensure that a user, choosing such a IaaS vendor specific element, always makes this choice with clear, unequivocal and complete understanding that it will technically limit or thwart switching and portability to another vendor.

At the moment, much of this approach is being done by implementing multiple open-source projects that are still active and rapidly innovating.  As such the needed standardisation activity is more at the governance of deployment of open-source projects and stabilisation of the project-to-project interoperability elements, such as the API calls between the components.

One can envisage standards that:

- Profile the required set(s) of open-source projects and/or open standards (e.g. Linux and Kubernetes)
- Set out common governance for updating projects, handling dependencies and back-wards compatibility and/or longevity of services, notice periods, user transfer processes etc.
- Stabilise the interoperability elements – where appropriate and in liaison with project communities.
- Ensure transparency about proprietary extensions and other proprietary elements.

In effect such ‘profile and governance’ standards would explicitly fit the definition of ‘functional equivalency’ as used in the Data Act.

This approach allows for computational work to be constructed in immutable packages (‘containers’ or web assembly’). These support the fundamental principles for architecting distributed systems, where work can be scheduled across versatile (think different CPU architectures, GPUs and servers from different manufacturers or services) available resources. The immutability approach gives rise to horizontal scaling and resilience.

The intent is to support the efforts to create a common software defined abstraction layer (virtualisation for compute, storage, networking etc) and support true distributed systems that can operate in a multi cloud vendor environment.

At the same time, recognise there are at least potential short-term advantages to proprietary offerings that optimise this process onto an underlying proprietary IaaS vendor.  Such IaaS/PaaS services should be transparent about the limitations and customers need to evaluate the long-term costs of either vendor dependency or recoding to switch vendors.

**Recommendation 12: IaaS standardization should be approached by proposing 'profile and governance' standards to define a common open-source / open standard abstraction layer and transparency requirements on proprietary extensions or alternatives.**