Cloud services market investigation

Technical barriers working paper

6 June 2024



This is one of a series of consultative working papers which will be published during the course of the investigation. This paper should be read alongside the Issues Statement published on 17 October 2023 and other working papers published.

These papers do not form the inquiry group's provisional decision report. The group is carrying forward its information-gathering and analysis and will proceed to prepare its provisional decision report, which is currently scheduled for publication in September/October 2024, taking into consideration responses to the consultation on the Issues Statement and responses to the working papers as well as other submissions made to us. Parties wishing to comment on this paper should send their comments to CloudMI@cma.gov.uk by 27 June 2024.

© Crown copyright 2024

You may reuse this information (not including logos) free of charge in any format or medium, under the terms of the Open Government Licence.

To view this licence, visit www.nationalarchives.gov.uk/doc/open-governmentlicence/ or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk. The Competition and Markets Authority has excluded from this published version of the working paper information which the inquiry group considers should be excluded having regard to the three considerations set out in section 244 of the Enterprise Act 2002 (specified information: considerations relevant to disclosure). The omissions are indicated by [%].

Table of Contents

Clo	oud services market investigation	0
1.	Summary	6
	Multi-cloud	6
	Switching	7
	Mitigations and incentives	8
	Potential remedies	9
2.	Introduction	. 10
	Approach to evidence gathering and analysis	. 10
3.	Background	
	Core services and ancillary services and tools	. 12
	Technical costs when using the public cloud	. 13
	Multi-cloud costs	. 13
	Switching costs	. 13
	Integrating multiple public clouds	. 15
	Potential sources of technical costs	. 15
4.	Technical multi-cloud and switching costs	. 17
	Multi-cloud costs	. 17
	Views of cloud providers	. 17
	Views of customers and other parties	. 18
	Switching costs	
	Technical costs involved in switching between clouds	. 21
5.	Core services: evidence on sources of technical cost	. 25
	Feature differentiation	. 25
	Evidence	. 26
	Our emerging views	. 29
	Interface differentiation	. 30
	Evidence	. 30
	Our emerging views	. 34
	Asymmetry of integrations	. 34
	Ofcom findings	. 35
	Our initial assessment	. 37
	Other views	. 38
	Our emerging views	
6.	Ancillary services and tools: evidence on sources of technical cost	. 41
	Common themes	.41
	Potential mechanisms for impact on customers' ability to multi-cloud or swi	tch
	Evidence from parties on the technical costs associated with ancillary servi	
	and tools	. 42
	Our emerging views	
	Identity and access management	
	General impact of IAM on customers' ability to multi-cloud and switch	. 44
	Impact of identity authentication on customers' ability to multi-cloud and	
		. 45
	Impact of access authorisation on customers' ability to multi-cloud and swit	ch
	Microsoft's IAM software and services	. 48

	Our emerging views	
	Billing	
	Impact of billing on customers' ability to multi-cloud and switch	
	Our emerging views	
	Observability	
	Impact of observability on customers' ability to multi-cloud and switch	
	Our emerging views	
	Provisioning and orchestration	
_	Our emerging views	
7.		
	Latency	
	Our emerging views	
	Skills	
	Our emerging views	
	Transparency	
	Our emerging view	
8.	Mitigation of technical costs to multi-cloud and switching	
	Current mitigations to technical costs	
	Existing mitigations to technical challenges	. 66
	Use of cloud providers' services designed to facilitate multi-cloud and/or	
	switching	
	Use of customer-led mitigations to technical challenges	. 70
	Use of provider-led mitigations to technical challenges	
	Our emerging views	. 77
	Cloud providers' incentives to compete on mitigating technical challenges	. 78
	Evidence from cloud providers	
	Our initial assessment	. 80
9.	Potential remedies	. 83
	Introduction	. 83
	Overview of potential remedies to technical barriers	. 83
	General design considerations for potential remedies to technical barriers	. 84
	Cloud services and/or interfaces that would be in scope	. 84
	Cloud providers that would be in scope	. 84
	Duration	
	Interactions with regulations outside the UK	. 85
	Remedies requiring cloud providers to increase standardisation	
	Potential remedies that require common standards for cloud providers	
	General category of cloud service or interface	
	Extent to which common standards have been adopted	. 87
	Potential remedies that use principles-based requirements	
	Potential remedy to improve the interoperability of cloud services through the	
	use of abstraction layers	
	Potential for unintended consequences	
	Potential remedies to increase interconnectivity and reduce latency	
	Potential remedy that involves connecting third party data centres	
	Potential remedy that requires cloud providers to make data centre space	
	available for other cloud providers	98
	Remedies requiring cloud providers to be more transparent about the	
	interoperability of their cloud services	99
	Stakeholder views	

Remedy requiring cloud providers to publish documentation on the	
interoperability of cloud services and the ability to migrate away from clo	ud
services	100
Remedy requiring cloud providers to give notice and publish details of	
upcoming material updates to cloud services	101
Remedies to improve skills	103
Require cloud providers to make training and education courses cloud-	
agnostic	103
Summary of potential remedies and invitation to comment	104

1. Summary

- 1.1 This working paper presents our initial analysis of the potential impact of technical barriers on public cloud customers' ability and incentive to switch and multi-cloud and whether they limit competition between cloud service providers.
- 1.2 For this analysis, we have considered the following:
 - (a) the technical barriers that customers face when using multiple public clouds and switching between public clouds, as well as any impact these have on their behaviour; and
 - (b) any mitigations that reduce these barriers, as well as cloud providers' incentives to reduce them.
- 1.3 The focus of our evidence-gathering has been mostly on customers because they are best placed to provide evidence on the technical barriers they face when switching between multiple public clouds and/or integrating them and the extent to which this affects their behaviour. We have also heard from a range of other parties, including cloud providers, independent software vendors (ISVs) and industry bodies.
- 1.4 Interpreting evidence from customers has been complex because they are highly heterogenous: they vary broadly in terms of their technical sophistication, the stages they are at in their cloud journey, the types of workloads they have on public cloud, the number of staff they have and the extent of their use of the cloud. Each of these factors influences their behaviour.
- 1.5 We set out our emerging views based on the evidence we have seen to date and our initial thinking on potential remedial action if any adverse effect on competition is found.

Multi-cloud

1.6 The evidence we have seen to date relating to technical barriers when using multiple public clouds presents a varied picture. Some customers mentioned general concerns about the difficulty of integrating and operating multiple clouds, including issues such as additional complexity, operational overheads and the differences between clouds. However, some customers said that they

face minimal challenges due to the availability of open APIs,¹ cloud-agnostic ISV services and other workarounds.

- 1.7 We were also told about some specific factors that contribute to technical barriers customers face when integrating and operationalising multiple public clouds:
 - (a) the differences in interfaces of core services;
 - (b) the differences between how certain cloud infrastructure services integrate with other services from the same cloud provider and how they integrate with ISVs' services (ie asymmetry of integrations);
 - (c) the differences in interfaces of ancillary services and tools and in particular Identity and Access Management (IAM) services and tools;
 - (d) the differences in skills required to operate and engineer within different public clouds; and
 - (e) the latency of connections between different public clouds.

Switching

- 1.8 The evidence we have seen to date relating to technical barriers when switching presents a clear picture: it shows that customers experience technical challenges relating to switching between public clouds, and this can affect their willingness to consider switching and the extent to which switching takes place.
- 1.9 Some customers described in general terms the technical barriers to switching that they faced and the associated lock-in, such as the time and effort required to re-design and re-engineer their workloads due to the technical differences between clouds.
- 1.10 If the customer moves only part of a workload, or other workloads remain on public clouds other than the target cloud, this will introduce a multi-cloud architecture, which may lead to that customer experiencing the barriers to using such an architecture that are set out above.
- 1.11 We were also told about some specific factors that contribute to technical barriers to switching:

¹ An API is an application programming interface. By 'open API' we mean APIs that can generally be accessed by any party.

- (a) the differences in features and interfaces of core services, particularly in Platform as a Service (PaaS)²;
- (b) the differences in features of ancillary services and tools, and in particular in IAM services and tools;
- (c) the differences in skills required to operate and engineer within different public clouds.

Mitigations and incentives

- 1.12 The evidence we have seen to date shows that customers must invest extra effort and resources to mitigate lock-in. Customers consider this as a trade-off when deciding their cloud strategy: some view lock-in as being necessary to gain the benefits of the cloud (eg to use highly abstracted, proprietary, managed PaaS services), whereas other customers prioritise reducing lock-in as much as possible (eg by deploying and managing their own cloud-agnostic software).
- 1.13 Whilst some specific software, such as Kubernetes and Terraform, as well as proprietary services such as Azure Arc, may help customers use more than one cloud, such software does not fully overcome the challenges of using multiple public clouds and switching between them.
- 1.14 The large cloud providers, AWS and Microsoft, told us that they are incentivised to make their public clouds interoperable in order to retain customers that value avoiding a lock-in and/or win such customers from competing providers.
- 1.15 However, it does not necessarily follow that just because customers would value interoperability between public clouds, cloud providers are incentivised to lower technical barriers for multi-cloud and switching. While lowering such barriers may allow cloud providers to win more incremental customers and/or workloads from their rivals, it may also increase the risk that these cloud providers lose customers and/or workloads to their rivals, or that these cloud providers would have to offer more competitive prices, quality or levels of innovation in order to retain them.
- 1.16 Overall, cloud providers face a complex mix of incentives when deciding whether or not to support multi-cloud and switching. Therefore, in assessing cloud providers' incentive to lower technical barriers to multi-cloud and switching, we will consider the extent to which efforts to facilitate

² See Paragraph 3.3 for a definition of PaaS.

interoperability have already eliminated technical barriers or, conversely, to what extent technical barriers remain.

Potential remedies

- 1.17 If any adverse effects on competition are found in relation to technical barriers, potential remedies include those which could require cloud providers to:
 - (a) increase the degree of standardisation of cloud services and/or interfaces, to increase interoperability and portability of cloud services, through voluntary standards, mandatory standards, or principle-based requirements;
 - (b) improve the interoperability of cloud services, through the use of abstraction layers;
 - (c) increase interconnectivity and reduce latency;
 - (d) increase transparency around the interoperability of cloud services; and/or
 - (e) improve the portability of skills between cloud providers.
- 1.18 In assessing potential remedies, we will consider their effectiveness and proportionality, as well as considering their potential effects both positive and negative on those parties most likely affected. This will include assessing the extent to which there are any relevant customer benefits that are foregone as a result of a remedy.

2. Introduction

2.1 This working paper sets out our initial analysis of the potential impact of technical barriers on public cloud customers' ability and incentive to switch and multi-cloud, and whether they limit competition between cloud service providers.

Approach to evidence gathering and analysis

- 2.2 In order to assess whether there are technical barriers that impact customer behaviour or are likely to do so, we asked a range of questions to customers, cloud providers, ISVs, suppliers of professional services, industry bodies and non-profit organisations. We have also reviewed similar evidence collected by Ofcom.
- 2.3 In line with the qualitative nature of this evidence, we have set out a summary of the key points we consider emerging from the evidence in the round, noting that no one question is determinative of any issue. Where appropriate we set out additional context and relevant factors that we are taking into account in interpreting this evidence.
- 2.4 We also commissioned separate qualitative research from Jigsaw Research.³ This research was intended to capture a wider range and a different set of customers from those we engaged with directly. We have included some of this evidence in this working paper and will continue to analyse this research alongside the other evidence outlined in this paper, as well as any further relevant evidence received.
- 2.5 Our issues statement set out a theory of harm that 'technical barriers make switching and multi-cloud harder and limit competition between cloud providers'.⁴ We are investigating whether, and to what extent, technical barriers prevent or restrict the ability of customers to:
 - (a) adopt and use a multi-cloud architecture, particularly integrated multi-cloud; and/or
 - (b) switch, particularly between public clouds.
- 2.6 We consider whether there are any specific factors from which technical barriers arise, or sources of technical costs that increase the effort required from customers to use a multi-cloud architecture or switch. In particular, we look at sources of technical costs in the core cloud infrastructure services that

³ Cloud Services Market Investigation Qualitative Customer Research conducted by Jigsaw (2024).

⁴ CMA Issues Statement on the Cloud Services Market Investigation, paragraphs 22-25.

contribute to the key objectives of the workload, in ancillary services and tools (ie those that support core cloud infrastructure services), and in other related factors, specifically latency, transparency and skills.

- 2.7 We are examining the extent to which technical barriers can be overcome by customers and the extent to which they are inherent in the technology.⁵ In doing so, we are considering whether the mitigations available to customers are effective, given their potential costs and benefits, and whether any technical barriers that are inherent can nevertheless be reduced through mitigations.
- 2.8 Parties wishing to comment on this paper should send their comments to CloudMI@cma.gov.uk by 27 June 2024.

⁵ CMA Issues Statement on the Cloud Services Market Investigation, paragraphs 22-25.

3. Background

3.1 In this section we set out the concepts we have used to structure our analysis in this working paper.

Core services and ancillary services and tools

- 3.2 For the purposes of this working paper, we distinguish between what we have named 'core services' and 'ancillary services and tools'. This distinction informs our analysis because we think that the impact of technical multi-cloud or switching costs could be different between these two categories.
- 3.3 Core services are the main Infrastructure as a Service (IaaS)⁶ and PaaS⁷ services that contribute to the key objectives of the customer's workload.
- 3.4 Ancillary services and tools provide functions that support the operation and management of core services. They include:
 - (a) IAM: ancillary services and tools that allow customers to control who (person or application) can access what they have in the cloud. IAM is part of the broader category of security services and tools.
 - (b) Billing: the mechanisms used to monitor, analyse, and charge for cloud services. The tools used in cloud billing help customers monitor usage costs, forecast spending and identify opportunities for savings.
 - (c) Observability: the process of measuring, analysing and visualising the current state of a customer's cloud architectures based on the data it generates, such as logs, metrics, and traces. This can be used to identify the location and causes of bugs in applications and workflows.
 - (d) Provisioning and orchestration: the process of automating the tasks needed to manage deployment, connections and operations of workloads. Cloud orchestration technologies integrate automated tasks and processes into a workflow to perform specific business functions.

⁶ IaaS are cloud services that provide access to raw computing resources (compute, storage, and network) for processing workloads and storing data. The hardware associated with these computing resources take the form of servers and networking equipment owned and managed by the IaaS provider (and typically held on racks in a remote data centre). To allow and manage that access, IaaS also includes some necessary software, including networking and virtualisation.

⁷ PaaS are cloud services that provide access to a virtual environment for customers to develop, test, deploy and run applications. They include application development computing platforms and pre-built application components and tools which customers can then use to build and manage full applications.

Technical costs when using the public cloud

- 3.5 Technical barriers are costs to customers that can arise from the technical aspects involved when they switch between or use multiple clouds. These technical costs for customers can include spend, time, use of resources, engineering effort, operational risk and complexity.
- 3.6 In some cases, customers may be prepared to incur the costs involved to overcome technical barriers in order to realise the perceived benefits of doing so. In others, customers may be deterred by these costs from switching or using multiple clouds. In both cases, if ways can be found to lower or remove these technical costs, the barriers to switching or multi-clouding may be reduced.

Multi-cloud costs

3.7 Customers may incur two types of multi-cloud costs: operational costs and integration costs.

Operational costs

3.8 Customers may incur technical costs when operating workloads on more than one public cloud, independently of the level of integration between the workloads. Our definition includes only the additional operational costs incurred when using more than one cloud, noting that operating any single cloud requires some effort. For example, a customer may expend additional engineering effort to align its use of ancillary services and tools across clouds, or to reconcile different billing systems.

Integration costs

3.9 Customers may incur technical costs when enabling workloads on multiple public clouds to communicate. This may include setting up connections over a network using service APIs, as well as any ongoing management and operation of any integrations. The level of integration between workloads can vary and we consider this in the following subsection.

Switching costs

- 3.10 Customers may incur technical costs when switching workloads that exist on one public cloud (ie origin cloud) to another (ie target cloud). This may include:
 - (a) redesigning the workload such that it can be run on the target cloud;

- (b) setting up and operationalising services on the target cloud;
- (c) moving relevant data from the origin cloud to the target cloud; and
- (d) testing the new workload on the target cloud before switching it off on the origin cloud. This step can involve a multi-cloud architecture, which may incur temporary multi-cloud costs as set out above.
- 3.11 If the customer moves only part of a workload, or other workloads remain on public clouds other than the target, this will also introduce a multi-cloud architecture, which may also incur multi-cloud costs as set out above.
- 3.12 Our analysis has focused on the ability of customers to switch between and use multiple public clouds, therefore we have not examined initial migration costs from on-premises to the public cloud.

Figure 3.1: The technical costs associated with different customer activities and multi-cloud approaches



Source: CMA

Integrating multiple public clouds

- 3.13 Customers can integrate their use of multiple public clouds in many ways, with varying services, architectures and levels of interdependence involved. However, we have identified some broad categories of integration lying on a spectrum.
- 3.14 Completely siloed: in a completely siloed architecture, there are no interdependencies at all. With such an architecture we would expect a customer's clouds to be completely independent and a complete lack of communication between clouds.
- 3.15 Integration for management: at this level of integration there is some integration of the clouds for management purposes. This might look like connecting all a customer's clouds together with a network so that workloads may see each other, or a shared observability service which is responsible for logging analytics across clouds. Whilst this could be considered a 'low level of integration' it might still include transfers of significant amounts of data.
- 3.16 Integration between applications: at this level of integration there is some light interdependence between related workloads. This might look like an operational workload on one cloud that generates data in relation to customers, which is then transferred to an analytical workload on another cloud for insights.
- 3.17 Integration within an application: at this level of integration, workloads that contribute to the same application or share overall objectives are integrated to work together in an application. This might look like a website hosted on one cloud which is heavily dependent on a database with customer data hosted on another cloud.
- 3.18 Integration within workloads: integration within workloads is the highest possible level of integration and consists of splitting 'one workload' across clouds. We did not identify many customers using this architecture, although this may be because one interpretation of a 'workload' could be the smallest discrete chunk of work to run on a single cloud and therefore may not be how customers would describe their architecture.

Potential sources of technical costs

3.19 The evidence we have received to date has highlighted a number of sources of technical switching and multi-cloud costs. These can be grouped into those that relate to the way cloud infrastructure services are designed and those that do not.

- 3.20 Service-design-related sources of technical costs include:
 - (a) differentiation of functionality: differences in the functionality of similar cloud infrastructure services hosted on different public clouds;
 - (b) differentiation of interfaces: differences in the interfaces (eg protocols or APIs) of similar cloud infrastructure services hosted on different public clouds; and
 - (c) asymmetry of integrations: a lack of ability to directly integrate first-party public cloud infrastructure services with services from third parties hosted on the same or a different cloud to the same extent as when integrating with other first-party public cloud infrastructure services.
- 3.21 Other sources of technical costs include:
 - (a) latency: the time it takes to transfer data between public clouds. A relevant factor when considering integrating between multiple public clouds, but also when customers need to move data across regions and/or availability zones;
 - (b) skills: the difference in technical skills needed to work with different public clouds; and
 - (c) transparency: the availability and discoverability of information about potential technical challenges.

4. Technical multi-cloud and switching costs

- 4.1 In this section we consider the evidence we have seen to date about the existence of technical multi-cloud and switching costs, and any impact of these on customer behaviour.
- 4.2 We focus on customers' experiences of the technical aspects of attempting to switch public clouds or use and integrate multiple public clouds. Evidence from other stakeholders, such as cloud providers, ISVs and industry bodies is also included where relevant.
- 4.3 Some customers and an organisation we spoke to said that technical effort to switch and use multiple clouds stems from the fundamental differences in how each of the public clouds have evolved over time.⁸ They pointed to differences in approaches, APIs, technical implementations, tools, frameworks, methodologies and best practices. This may have implications for how feasible it would be to attempt to resolve deep-rooted differences in fundamental constructs and philosophy across clouds and we will consider this further in our ongoing analysis of potential remedies.

Multi-cloud costs

4.4 In this section, we consider the potential technical costs relating to the integration of multiple clouds between applications, within applications and within workloads, as well as integration for the purpose of management. We also consider any operational costs relating to these architectures.

Views of cloud providers

- 4.5 Google said it believes there is real customer appetite for integrated multicloud strategies, and that integration between multiple clouds is more likely to be adopted for cloud-native⁹ workloads. It said that digital native customers who do not have a historical reliance on legacy on-premises software products, are well-positioned and more likely to adopt multi-cloud strategies. It said that in contrast, traditional enterprises across all sizes and sectors often find an integrated multi-cloud set-up more challenging.¹⁰
- 4.6 However, two cloud providers said that there are operational challenges that disincentivise customers from using a multi-cloud approach:

⁸ Responses to CMA's information requests [\times]; [\times] submission to Ofcom [\times]; Note of meeting with [\times].

⁹ 'Cloud-native workloads' refers to workloads created on the cloud, not migrated from on-premises.

- (a) AWS said that operational challenges include increased data latency, data governance issues, security and data privacy issues due to managing multiple IT environments. It said that these operational challenges are inherent to integrating multiple IT environments and are not caused by any issues specific to or restrictions imposed by cloud providers.¹¹
- (b) Microsoft said that integrated multi-cloud gives customers the ability to use services from different cloud providers, but is generally the least preferred approach by customers. This is because it increases the complexity of building, maintaining and securing applications and also creates multiple points of failure across different clouds. Therefore, customers will typically only choose this model where there is a particularly differentiated service that represents a unique value proposition for their needs.¹²

Views of customers and other parties

The extent to which customers integrate multiple clouds

- 4.7 The extent to which customers are integrating between clouds, and the methods with which they do so, provides useful context to interpret the evidence relating to any associated technical costs. Further to our analysis of the prevalence of the use of multi-cloud in our competitive landscape working paper, in which our emerging view was that there is some degree of multi-cloud, but it may be quite limited in scope and mostly found in relation to larger customers,¹³ we set out the evidence we have seen to date from customers relating to this below.
- 4.8 Some customers said that they integrate between multiple public clouds for the purpose of management, by integrating their ancillary services, such as IAM. We consider the technical costs of doing so in greater depth in section 6.¹⁴
- 4.9 Evidence from other customers shows that they are integrating or communicating between applications on different public clouds,¹⁵ for example by building intermediary integration layers that connect cloud networks, using open APIs, and connecting between the storage services of multiple cloud providers. We understand that these customers tend to integrate only

¹¹ AWS' response to CMA's information request [>].

¹² Microsoft's response to CMA's information request [>].

¹³ Competitive landscape working paper (publishing.service.gov.uk) See also 'Integrating multiple public clouds' in section 3 for more information about the extent to which customers can integrate multiple public clouds.

¹⁴ Responses to CMA's information requests [>].

¹⁵ Responses to CMA's information requests [\gg].

between the storage services of multiple clouds, rather than directly between features of other services.

4.10 Another group of customers also told us they are, or have experimented with, integrating within applications and/or workloads across multiple public clouds. This includes using services with cross-cloud elements (such as querying the storage service on one cloud from a data warehouse service on another cloud), in addition to connecting only between the storage services.¹⁶

Technical costs involved in integrating and operating multiple clouds

- 4.11 Evidence we have seen to date shows that most customers face additional technical costs to operate more than one public cloud, whether or not they choose to integrate their use of them.¹⁷
- 4.12 The evidence relating to the technical costs that customers incur when integrating multiple public clouds is mixed, consistent with our view that customers are heterogenous. A supplier of professional services said that the barriers a customer would face in adopting multi-cloud would depend on its individual workloads and connectivity requirements.¹⁸
- 4.13 Some customers, ISVs and a supplier of professional services told us that there are challenges to integrating within applications and/or workloads across multiple clouds.¹⁹ A subset of these customers said that although there are challenges, there are some workarounds such as using third party tools or building custom solutions to connect services.²⁰
- 4.14 Responses from other customers showed that they experienced minimal barriers to integration across multiple public clouds.²¹ Reasons given for this included the availability of open APIs that make integration easier, workarounds provided by third parties and integrations that are enabled and/or documented by cloud providers.
- 4.15 Some customers said that they reviewed the option to integrate public clouds, but concluded that the benefits did not outweigh the technical costs of doing so for their current use cases.²² Other customers said that they viewed the

¹⁷ Responses to CMA's information requests [\gg]; Notes of meetings with [\gg].

¹⁶ Due to differentiation in interpretation of the term 'workload', we have grouped responses that related to integrating within applications and workloads, as we understand the difference between the two approaches to be of no consequence for our analysis. Responses to CMA's information requests [\approx]; Notes of meetings with [\approx].

¹⁸ Note of meeting with [>].

¹⁹ Responses to CMA's information requests [\gg]; Notes of meetings with [\approx].

²⁰ Responses to CMA's information requests [%]; Notes of meetings with [%].

²¹ Responses to CMA's information requests [\gg]; Notes of meetings with [\gg].

²² Responses to CMA's information requests [\times]; Note of meeting with [\times].

benefits of integrating multiple clouds as being too low, but didn't mention whether this was in comparison to the technical costs.²³

- 4.16 Similarly, the Jigsaw report found that there are very significant technical barriers that reduce customers' willingness to consider multi-cloud, and that many customers do not see a strong argument for a multi-cloud strategy.²⁴
- 4.17 However, given the evidence set out in the previous sub-section, some customers are integrating both between and within applications across multiple public clouds, therefore this suggests they saw at least some benefit to doing so. Furthermore, some customers said that multi-cloud is a part of their business strategy,²⁵ and others said whilst they don't currently have a use-case for integrated multi-cloud, they may do so in the future.²⁶
- 4.18 Customers' decisions about where to place workloads that relate to each other are highly relevant to our analysis. Such workloads are more likely to be used by the same team or business unit and their integration is more likely to be desirable or necessary. Therefore, the easier it is to operate and integrate workloads across multiple public clouds, the more we might expect to see customers placing related workloads on different public clouds.
- 4.19 Evidence we have seen to date shows that customers tend to put related workloads on the same public cloud, in order to, for example, reduce operational complexity and prevent a reduction in resilience.²⁷
- 4.20 A customer said that when utilising a multi-cloud strategy, consideration must be applied to risks associated with a business process traversing multiple cloud providers, to prevent the impact of a single cloud provider failure from introducing increased operational resilience risk to the business process.²⁸ We understand this to mean that the addition of a second public cloud could double the likelihood that an application fails, if that application were designed in a way that a service outage of either of the public clouds it is dependent on would impact it.
- 4.21 This is consistent with evidence received from some cloud providers.²⁹

²³ Responses to CMA's information requests [\succ].

²⁴ Cloud Services Market Investigation Qualitative Customer Research conducted by Jigsaw (2024), paragraph

^{4.5.8.}

²⁶ [\times] response to CMA's information request [\times]; Note of meeting with [\times].

²⁷ [\times] response to CMA's information request [\times]; Notes of meetings with [\times].

²⁸ Note of meeting with [>].

²⁹ Responses to CMA's information requests [\times].

- 4.22 However, another customer said it had been able to avoid this challenge by designing its application such that a user's experience would not immediately be affected if either cloud stopped operating.³⁰
- 4.23 A customer told us that it is flexible in placing new workloads due to the benefits of using multiple public clouds.³¹

Switching costs

4.24 In this section, we consider the potential switching costs for customers moving workloads from one public cloud to another.

Technical costs involved in switching between clouds

- 4.25 The evidence we have seen shows that many customers anticipate or experience significant technical costs to switch public clouds.³² Customers described the costs as significant either in absolute terms eg a customer said 'it would take 12 months and tie up approximately 1,000 employees',³³ or in relative terms eg some customers described technical barriers as the main barrier to switching.³⁴
- 4.26 Some of these customers indicated that these costs had stopped them from switching or considering switching.³⁵ A customer said that the cloud providers are continually innovating such that it is not possible to determine which one will be superior in a year's time. It said that even if its cloud provider raised all its prices by 5%, this would not be enough of a driver to move everything to a competitor.³⁶ This customer also said that a switch would cost a similar amount to the initial migration.³⁷
- 4.27 Similarly, the Jigsaw report found that there are technical barriers that significantly reduce customers' willingness to consider switching cloud provider.³⁸

³¹ Note of meeting with [>].

³² Responses to CMA's information requests [%]; Notes of meetings with [%].

³³ Note of meeting with [>].

³⁴ Responses to CMA's information requests [\gg]; Notes of meetings with [\gg].

 $^{^{35}}$ Notes of meetings with [>].

 $^{^{36}}$ Note of meeting with [><].

³⁷ [\gg] response to CMA's information request [\gg].

³⁸ Cloud Services Market Investigation Qualitative Customer Research conducted by Jigsaw (2024), paragraph 4.5.8.

- 4.28 Some customers and other market participants (eg professional services suppliers) view AWS, Microsoft and Google as having broadly equivalent offerings, in terms of products, features and prices.³⁹ For example:
 - (a) A customer said that the capability gap between the 'three main hyperscalers' is much reduced now compared to five years ago, and there is little to choose between them outside of some speciality areas and niche use cases.⁴⁰
 - (b) Other customers said that any innovations in one cloud provider's offerings are matched quickly by the others.⁴¹
 - (c) Another customer said that there are differences in functionality between laaS/PaaS on different clouds, but the question is whether they are significant enough to switch. It said that for laaS, the differences are not significant enough and for PaaS it comes down to developer preferences, which largely come from which platform they are familiar with using.⁴²
- 4.29 Where parties did mention differences in the offering of public cloud providers, they said that these are currently relatively minor or cover edge cases.⁴³
- 4.30 Some customers said that, given the similarity of the current offerings by cloud providers from their perspective, the value of switching is low in comparison to the costs.⁴⁴ Similarly, the Jigsaw report found that many customers do not see a strong argument in favour of switching.⁴⁵
- 4.31 Some cloud providers submitted that the technical differences between their public clouds result from their innovation which has been driven by competition in the market.⁴⁶
- 4.32 AWS said that IT providers offering proprietary services based on innovative and new technologies is not anti-competitive, adding that, in its view, the ability to profit from innovation is what incentivises competitors to provide new products that best meet their customers' needs. AWS said that stifling the development of innovative proprietary technologies in the name of interoperability or portability would harm competition by limiting the ability of,

⁴² Note of meeting with [>].

³⁹ Responses to CMA's information requests [\approx]; Notes of meetings with [\approx].

⁴⁰ [\times] response to CMA's information request [\times].

⁴¹ Note of meeting with [\times]; [\times] response to CMA's information request [\times].

⁴³ Notes of meetings with [\times]; Responses to CMA's information requests [\times].

⁴⁴ Notes of meetings with [\times]; Responses to CMA's information requests [\times].

⁴⁵ Cloud Services Market Investigation Qualitative Customer Research conducted by Jigsaw (2024), paragraph 4.5.8.

⁴⁶ AWS' response to the Issues Statement, 17 October 2023, paragraphs 18 and 22; [≫] submission to CMA [≫]; Microsoft's response to the Issues Statement, 17 October 2023, paragraphs 23-25; Google's response to the Issues Statement, 17 October 2023, paragraphs 3, 10-11 and 18-19; and Oracle's response to the Issues Statement, 17 October 2023, pages 1-2.

and incentive for, IT providers such as AWS to create solutions that best support their customers' needs. In AWS' view, when IT providers develop service features that integrate with their other proprietary services they can drive competition on service quality differentiation, further increasing incentives to innovate. AWS said that allowing IT providers to release features before they are fully interoperable allows them to get new technology to market quickly, which can further spur rival innovation from their competitors.⁴⁷

- 4.33 Microsoft said that cloud providers invest heavily in innovation to differentiate themselves, which brings inevitable complexity to customers' cloud architecture. It added that new cloud services may be inherently less interoperable or portable, if they are the result of technical innovation which is either not available on all clouds or as a result of parallel innovation. Microsoft also said that differentiation can exist in the form of the cost, security features, scalability/agility, technology and performance, compliance features, sustainability and resilience of cloud infrastructure.⁴⁸
- 4.34 Oracle said that 'architectural engineering fundamentally differentiates some of the [cloud providers'] offerings'. It said that it has 'facilitated a multi-cloud strategy to help customers take advantage of each [cloud provider's] architectural innovations, even when that innovation creates fundamental differences in engineering'. Oracle said that '[a]rchitectural innovation targets the entire stack of technology used to deliver cloud services and can result in better performance, lower costs, higher security and a smaller environmental footprint for similar services'. It also said that it is differentiated from other cloud providers in part because it optimises for speed and performance.⁴⁹
- 4.35 Other cloud providers expressed different views from those above on the extent to which technical differentiation results from innovation and competition in the market.
- 4.36 Google said that to preserve competition and foster future innovation, it is critical for customers to have unconstrained ability to switch providers and adopt multi-cloud strategies.⁵⁰
- 4.37 IBM said that, while innovation increases the quality of service for customers, it may also increase technical switching barriers if improvements are only

⁴⁷ AWS' response to CMA's information request [\Join].

⁴⁸ Microsoft's response to the Issues Statement, 17 October 2023, paragraphs 23-25.

⁴⁹ Oracle's response to the Issues Statement, 17 October 2023, pages 1-2.

⁵⁰ Google's response to the Issues Statement, 17 October 2023, paragraphs 3, 10-11 and 18-19.

available to first-party services of a cloud provider [>], but not to competing third party services.⁵¹

- 4.38 OVHcloud agreed with Ofcom's assessment that justification for technical differentiation of cloud infrastructure services and cloud ancillary services, through proprietary technologies, is less clear.⁵²
- 4.39 We welcome views on the ways in which technical barriers may influence future competition, including price, quality, innovation and customer choice.

⁵¹ IBM's response to the Issues Statement, 17 October 2023, paragraph 3.2.

5. Core services: evidence on sources of technical cost

- 5.1 In this section we consider whether there are technical aspects of core services that increase the costs for customers when using multiple clouds or switching. As set out in section 3 of this paper, core services are the main laaS and PaaS services that contribute to the key objectives of the workload.
- 5.2 We set out the evidence in relation to three potential sources of technical switching and/or multi-cloud costs:
 - (a) feature differentiation;
 - (b) interface differentiation; and
 - (c) asymmetry of integrations.

Feature differentiation

- 5.3 In this sub-section, we present the evidence we have seen to date on the extent to which differences in features of comparable core services from different cloud providers result in technical switching and/or multi-cloud costs. We have considered two aspects:
 - (a) the functionalities of the service (ie what it does); and
 - (b) the implementation of these functionalities (ie how a service does it).
- 5.4 We expect that differences in core service features across clouds might have a more significant impact on a customer's ability to switch than their ability to use or integrate between multiple clouds. This is because customers tend to replicate the functionality of the original workload on the target cloud, which may lead to a need for services that have equivalent features across the original and target cloud. However, when using multiple clouds, the workloads on each are typically different and therefore there may be less need for equivalent features across clouds.
- 5.5 There are exceptions to this, for example customers operating in regulated environments, such as banking, which require a duplicated multi-cloud architecture. Such an approach would also require equivalent features across clouds.
- 5.6 Customers had mixed views on whether there are differences in the features of comparable core services across clouds that make it harder to use multiple clouds or switch. This may be because the particular services customers use have varying levels of differences in their features. Some customers explained

their views and gave evidence about differences in IaaS and PaaS services, whilst others did not.

Evidence

- 5.7 Some customers who we spoke to said that cloud providers offer similar features in their core services. Customers said that Microsoft and AWS increasingly offered equivalent services, though some noted that Google lagged behind in a few areas.⁵³
- 5.8 Some of these customers did not note any increase to the technical cost associated with switching or integrating multiple clouds coming from differences in the features of core services.⁵⁴ For example, a customer said that there was a general parity of services between providers and working with multiple providers was easy.⁵⁵
- 5.9 Some customers and other organisations said that many IaaS services are more similar across cloud providers in comparison to PaaS core services and did not note significant challenges to switching or multi-cloud in relation to IaaS services.⁵⁶
- 5.10 For example, a customer said that as a general matter, different cloud providers offer the same core services, such as compute and storage networking and therefore switching is not particularly difficult or costly but that some planning is required to deal with the intricacies across providers.⁵⁷
- 5.11 A supplier of professional services said that IaaS is functionally similar across some providers, but that all providers' services have their own intricacies.⁵⁸
- 5.12 An organisation said that basic laaS services and their features are similar across providers and easily portable.⁵⁹
- 5.13 However, some cloud providers said that there are differences in the features of core services. A few added that differences in features of core services from other clouds make switching and using multiple clouds more difficult.⁶⁰
- 5.14 For example, a cloud provider said some other providers use proprietary standards and code to make it very difficult for customers to switch certain

⁵³ Responses to CMA's information requests [%]; Notes of meetings with [%].

⁵⁴ Responses to CMA's information requests [\gg]; Notes of meetings with [\gg].

⁵⁵ Note of meeting with [>].

⁵⁶ Responses to CMA's information requests [\gg]; Notes of meetings with [\gg].

⁵⁷ [>] response to CMA's information request [>].

⁵⁸ Note of meeting with [>].

⁵⁹ Note of meeting with [>].

⁶⁰ Microsoft's response to the Issues Statement, 17 October 2023, paragraph 24; [\times] response to CMA's information request [\times].

workloads away from their infrastructure towards that of another provider or to impose artificial friction on customers' ability to share data between services running in different infrastructure environments, but it is possible for customers to work around challenges of this nature.⁶¹

- 5.15 Oracle said that there can be technical difficulties when facilitating integration with other clouds. In particular, cloud providers' use of different standards or implementations can create difficulty as they can necessitate additional work or rework to implement and maintain a solution.⁶²
- 5.16 In addition, many customers and other organisations detailed how differences in features increased the technical cost of switching. They explained that whilst cloud providers may offer services with equivalent functionality in many cases, there were still differences which necessitated planning, remapping and reworking workloads when switching.⁶³
- 5.17 For example, a customer said that the features of core services are broadly similar in concept, but very different in detailed implementation and that this had a significant impact on the cost of switching and integrating clouds. It said that even the simplest workloads take more than a month to port, and the most complex can take over a year.⁶⁴
- 5.18 An ISV said that one area where there would be significant reworking is in AWS' DNS service – Route 53. In this ISV's view, Microsoft does not have an analogous service and therefore a move from AWS to Azure would require a substantial re-engineering of code.⁶⁵
- 5.19 OVHcloud said that the diversity of cloud providers' offers can also slow the migration towards an alternative cloud provider. It also said that, though the majority of the services and functionalities offered by cloud providers are very much alike, they can slightly differ from one another and make it difficult to replace one by another.⁶⁶
- 5.20 Many customers and other organisations also identified proprietary PaaS services as having more significant differences in features between cloud

⁶¹ [>] response to CMA's information request [>].

⁶² Oracle's response to CMA's information request [\gg].

⁶³ Responses to CMA's information requests [\approx]; Notes of meetings with [\approx]; Oracle's response to the Issues Statement, 17 October 2023, paragraph 2; Company A's response to the Issues Statement, 17 October 2023, paragraph 3.2; [\approx] submission to CMA [\approx].

⁶⁴ [\times] response to CMA's information request [\times]; Note of meeting with [\times].

⁶⁵ Note of meeting with [>].

⁶⁶ OVHcloud, submission to CMA [\gg].

providers than IaaS services. These customers and others detailed how these differences would increase the technical cost of switching.⁶⁷

- 5.21 For example, a customer said that cloud native services, which includes most PaaS, are not standardised, and may have different features that are not compatible or interoperable with other providers. Therefore, applications and data that are developed and deployed on one provider may not be easily ported or transferred to another without modification or adaptation.⁶⁸
- 5.22 Another customer said that Google's Big Query service uses a particular type of SQL and so if a company wanted to migrate to Amazon Redshift, it would have to conduct some SQL conversion, as an example of engineering effort required to migrate.⁶⁹
- 5.23 A supplier of professional services said that customers do not consider the proprietary nature of PaaS services, and once they have built an architecture based on all of these things, unpicking it and trying to integrate it across multiple clouds then becomes a very large task.⁷⁰
- 5.24 An organisation also said that there are more differences in the features of newer core PaaS services and in particular, Function as a Service (FaaS) is an area where providers have very divergent approaches and portability is difficult.⁷¹
- 5.25 Managed open-source services are a type of core PaaS service.⁷² A few organisations said there are differences in features of managed versions of the same open-source software across different clouds, which may make it more challenging to switch or use multiple clouds.⁷³
- 5.26 For example, a supplier of professional services said that providers package open-source tools to effectively make them into PaaS services and make it challenging to use them across clouds.⁷⁴

⁶⁷ Responses to CMA's information requests [\approx]; Notes of meetings with [\approx]; IBM's response to the Issues Statement, 17 October 2023, paragraph 1.6.

⁶⁸ [\times] response to CMA's information request [\times]; Note of meeting with [\times].

⁶⁹ Note of meeting with [>].

⁷⁰ Note of meeting with [>].

⁷¹ Note of meeting with [>].

⁷² Cloud providers offer management of open-source software as a service. Typically, the cloud provider will take responsibility for configuring, managing and running a piece of open-source-software. For example, AWS offers AWS Elastic Kubernetes Service which allows customers to use Kubernetes while AWS configures it, scales it and integrates its other services.

⁷³ [\times] response to CMA's information request [\times]; Notes of meetings with [\times]; IBM's response to the Issues Statement, 17 October 2023, paragraph 1.6.

⁷⁴ Note of meeting with [>].

- 5.27 A cloud provider said that, in its view, the lack of governance of open-source standards can lead to the creation of forked proprietary versions⁷⁵ of standards, reducing openness and interoperability.⁷⁶
- 5.28 As explained above, we expect differences in features of core services to have a less significant impact on customers' ability to use multiple clouds than on customers' ability to switch. However, a few customers, and other organisations also said that differences in features increased the technical cost of using multiple clouds.⁷⁷
- 5.29 For example, a customer said that there are circumstances where multiple providers offer identical solutions but that there are also situations where functional and non-functional differences exist which complicate the wider use of multiple clouds.⁷⁸
- 5.30 A supplier of professional services said that the implementation of IaaS services differs between clouds, including how connectivity, maintenance, monitoring, and patching is done. It said it is much simpler to consume services from a single cloud provider than across multiple cloud providers because it is more automated, more secure, more seamless and easier to scale. ⁷⁹

Our emerging views

- 5.31 Based on the evidence we have reviewed to date in relation to differences in core service features, our emerging view is that, while customers found that the large cloud providers offer generally similar features in their core laaS services, some customers found significant differences in the way the features of those services function. Some customers who solely used laaS services did not experience increased technical cost when switching or using multiple clouds, but others did.
- 5.32 The evidence also shows that some customers found significant differences in the features of large cloud providers' core PaaS services and experienced an increase in technical cost when switching, and to a lesser extent using multiple clouds, because of these differences.

```
<sup>76</sup> IBM's response to the Issues Statement, 17 October 2023, paragraph 1.6.
```

```
<sup>77</sup> Company A's response to the Issues Statement, 17 October 2023, paragraph 3.2; Responses to CMA's information requests [\gg]; Note of meeting with [\gg].
```

⁷⁵ An open-source fork is a project that has been derived from an existing open-source project but is now developed independently. Open-source licences typically don't restrict this and forks may have significant differences or be proprietary with more restrictive licenses.

⁷⁸ [\gg] response to CMA's information request [\gg].

⁷⁹ Note of meeting with [>].

Interface differentiation

- 5.33 In this sub-section, we present the evidence we have seen to date on the extent to which differences in interfaces of comparable core services from different cloud providers result in technical switching and/or multi-cloud costs.⁸⁰ For example, services may have different protocols or APIs that reduce substitutability or interoperability.
- 5.34 Cloud services typically use APIs, which are software interfaces that allow two or more pieces of software to communicate with each other and are the typical way of integrating workloads within or between clouds.
- 5.35 Customers largely found APIs to be differentiated across cloud providers but had mixed views on the impact of that on switching and using multiple clouds.

Evidence

- 5.36 Some cloud providers said that they offer open APIs for many of their services, which they said allow customers to easily switch and integrate multiple clouds even if there are differences in the APIs of different providers.⁸¹
- 5.37 However, a cloud provider said that integration between clouds would be easier if third parties were to publish their APIs/SDKs in the open so that they can be reviewed.⁸² It may be that there are some services for which large cloud providers do not publish open APIs, we invite stakeholders to raise any concerns they may have in relation to this.
- 5.38 Some customers and an organisation also said that APIs were differentiated for similar services across clouds.⁸³ But these organisations found integration using different but open APIs did not cause major challenges.⁸⁴
- 5.39 For example, a customer said that, though it is integrating between systems, it is doing so at the application level, using APIs, and that it does not find this to be a problem.⁸⁵

⁸⁰ When considering interfaces of cloud infrastructure services, we consider all aspects that may impact how a user interacts with a service, including APIs, protocols, and general workflows.

⁸¹ Microsoft's response to the Issues Statement, 17 October 2023, paragraph 30; [\times] submission to CMA [\times]; Responses to CMA's information requests [\times].

⁸² [\times] response to CMA's information request [\times].

⁸³ In practice this may mean the APIs use different syntax or a different underlying protocol, which are sets of standards that dictate how APIs communicate information across the internet.

⁸⁴ Responses to CMA's information requests [%]; Notes of meetings with [%].

⁸⁵ Note of meeting with [>].

- 5.40 Another customer said that it does not find differences in APIs to be an insurmountable challenge because it can use translation layers to convert between different clouds or have 'over-the-top'-par solutions that support multiple versions at once in a multi-cloud architecture.⁸⁶
- 5.41 An organisation said that generally differentiated APIs are not a technical blocker because workarounds are available.⁸⁷
- 5.42 Additionally, some customers said more generally that there are easy ways to integrate multiple clouds and that differences in interfaces were not a challenge to integration.⁸⁸
- 5.43 However, many other customers and organisations said that the differences in APIs of core cloud services across clouds were significant and detailed how they increased technical cost when integrating multiple clouds.⁸⁹
- 5.44 For example, a customer said that each cloud has different APIs and so it has to use third party tools to integrate them, as it is not as easy to have systems talk across clouds.⁹⁰
- 5.45 Another customer said differences in interfaces of core services necessitates extensive planning and testing.⁹¹
- 5.46 An organisation said that interoperability can also be undermined by providers changing their APIs frequently. It said that un-standardised APIs and the IP surrounding them, restricted the ability of third parties to develop software that integrates with the APIs.⁹²
- 5.47 A cloud provider said that there are very few cases where an API of a cloud provider has become a de facto standard for other cloud providers to use as well. It said almost every native capability and API required to instantiate and operate a workload across cloud providers is different.⁹³
- 5.48 The Jigsaw report also indicated that challenges due to inconsistent APIs and interfaces are among the most commonly raised by customers.⁹⁴

⁸⁶ [>] response to CMA's information request [>].

⁸⁷ Note of meeting with [>].

⁸⁸ Responses to CMA's information requests [\gg].

⁸⁹ Responses to CMA's information requests [\gg]; Notes of meetings with [\gg].

 $^{^{90}}$ [>] response to CMA's information request [>].

⁹¹ [\times] response to CMA's information request [\times].

⁹² Note of meeting with [\gg].

⁹³ [\gg] response to CMA's information request [\gg].

⁹⁴ Cloud Services Market Investigation Qualitative Customer Research conducted by Jigsaw (2024), paragraph 4.5.2.

- 5.49 Some customers, cloud providers and an ISV also said differences in the interfaces of core services increased the technical cost of switching by necessitating rework to recreate the integrations of a switched workload with other services or workloads.⁹⁵
- 5.50 For example, a customer said that a lot of testing and a careful cutover environment is necessary when switching because some APIs handle thousands of calls a day and many workloads depend on them. It also said that different interfaces would mean infrastructure as code and other software managing applications must be re-written when switching clouds.⁹⁶
- 5.51 Another customer said that the different interfaces of PaaS core cloud services mean that workloads cannot be easily ported without modification.⁹⁷
- 5.52 IBM said that differentiated APIs create technical barriers to workload migration which result in real costs in automation, code, networking, back-up, monitoring and operations.⁹⁸

Databases and storage services

- 5.53 The evidence suggests that generally APIs for core services are differentiated across clouds. However, it also suggests that the level of differentiation is not uniform across different types of services. In particular, a number of parties had differing views on the differences in interfaces of storage and database services, which are among the most widely used services across many customers and workloads.
- 5.54 We heard from customers and other organisations that there are differences in the interfaces of storage and database services across clouds and that these can create difficulties.⁹⁹
- 5.55 For example, a customer said that Amazon S3 is not a standard for data storage. Azure Blob Storage and S3 are very different with different SDKs and different APIs which means someone adapting software to both must effectively do the same work twice.¹⁰⁰

⁹⁵ Responses to CMA's information requests [\times]; [\times] submission to CMA [\times].

 $^{^{96}}$ Note of meeting with [><].

⁹⁷ [\gg] response to CMA's information request [\gg].

 $^{^{98}}$ IBM's response to CMA's information request [\times].

 $^{^{99}}$ Responses to CMA's information requests [\succ].

¹⁰⁰ Note of meeting with [>].

- 5.56 An ISV said it sees some challenges in dealing with different storage and database services since there are no standards for this. It gave the example of Amazon S3 and Azure Blob which do not have compatible APIs.¹⁰¹
- 5.57 OVHcloud said [\gg] and in some cases data portability may require a dedicated API, and the adaptation of the migrated data's format.¹⁰²
- 5.58 The Jigsaw report also indicated that challenges migrating databases and storage services are among the most commonly raised by customers and can necessitate rewriting database queries or other code.¹⁰³
- 5.59 However, some customers said that there are interfaces for storage and database which are common across clouds, especially for S3, and Postgres services, a type of open-source database. Some of these parties said the similar interfaces reduce the technical cost of using or switching these services across multiple clouds.¹⁰⁴
- 5.60 For example, a customer said the engineering effort required to move away from Amazon S3 would be low because it would just involve moving the data across. Similarly, a Postgres database would have a low engineering effort because it is the same data format across providers.¹⁰⁵
- 5.61 Another customer said that there are standard APIs for accessing S3 storage, and Amazon RDS Postgres and Cloud SQL Postgres which run the same underlying database.¹⁰⁶
- 5.62 Some cloud providers similarly said that they support some storage and opensource database services which have the same or similar interfaces across clouds.¹⁰⁷
- 5.63 For example, a cloud provider said that that one of its storage services is accessible from an S3-compatible API. It also said that its cloud also continues to support open-source database engines like MongoDB, MySQL, PostgreSQL and Redis.¹⁰⁸

¹⁰¹ Note of meeting with [>].

 $^{^{102}}$ OVHcloud, submission to CMA [\succ].

¹⁰³ Cloud Services Market Investigation Qualitative Customer Research conducted by Jigsaw (2024), paragraph 4.1.14 and 4.5.2.

¹⁰⁴ Responses to CMA's information requests [\gg]; Notes of meetings with [\gg].

¹⁰⁵ Note of meeting with [>].

¹⁰⁶ Note of meeting with [>].

¹⁰⁷ AWS' response to the Issues Statement, 17 October 2023, paragraph 19; Responses to CMA's information requests [×].

¹⁰⁸ [\times] submission to CMA [\times]; [\times] response to CMA's information request [\times].

- 5.64 Another cloud provider said that the Amazon S3 API had become a de facto standard for storage.¹⁰⁹
- 5.65 This evidence suggests that there may be some database and storage services with similar interfaces across clouds, and that the similar interfaces make it relatively easier to use or switch these services across clouds. However, some parties said that there are significant differences between the interfaces of some storage and database services.

Our emerging views

- 5.66 Based on the evidence we have seen to date, our emerging view is that the APIs of core services are differentiated between cloud providers.
- 5.67 There is some evidence to suggest that the extent of differences in interfaces varies between services, in particular, there were mixed views about the differences in interfaces in databases and storage, which are commonly used services.
- 5.68 The evidence also suggests that some customers experience difficulty when integrating multiple clouds due to the differences in APIs of core cloud services. The evidence was mixed on the degree of this impact. At least some customers also experienced technical costs when switching clouds due to these differences.

Asymmetry of integrations

- 5.69 A cloud infrastructure service by one provider often needs to interoperate with a cloud infrastructure service by another provider. This interoperability is not always technically possible, so will only enable partial functionality, unless another service by the first provider is used or a workaround is found. We use the term 'asymmetry of integrations' to describe these instances.¹¹⁰
- 5.70 In this subsection, we set out:
 - (a) Ofcom's findings of AWS and Microsoft services that have asymmetry of integrations, including the views of AWS and Microsoft;
 - (b) our initial view of Ofcom's findings;

¹⁰⁹ [\gg] response to CMA's information request [\gg].

¹¹⁰ In its market study, Ofcom referred to these cases as asymmetry of functionalities. Given the same functionality can be achieved through additional integrations, we have decided to rename this concept to asymmetry of integrations to better reflect the nature of the issue.

- (c) evidence on the impact of asymmetry of integrations on customers' ability to multi-cloud and switch; and
- (d) our emerging views.

Ofcom findings

5.71 In its market study, Ofcom identified several examples of asymmetry of integrations relevant to AWS and Microsoft services. We have set these out in the table below along with information that Ofcom had on the uptake of these services.

Table 5.1: Ofcom examples of A and Microsoft cloud services with potential interoperability limits

Supplier	Service	Uptake	Potential limits to interoperability ¹¹¹
AWS	Amazon Athena	[≫]. ¹¹²	Can only query data stored on Amazon S3.
AWS	Amazon IVS	This service is used by large companies such as GoPro. ¹¹³	Can only auto-record to Amazon S3.
AWS	Amazon Kinesis Video Streams	[≫]. ¹¹⁴	Can only deliver extracted images to Amazon S3.
AWS	Amazon Omics	AWS' website shows this service is popular with customers in the clinical space. ¹¹⁵	Uses Amazon S3 for data import and export.
AWS	Amazon Pinpoint	[≫]. ¹¹⁶	Allows adding Amazon Personalize recommendations to a marketing email campaigns, but not from third party recommendations engines.
AWS	Amazon RedShift	\$[≫] ([≫]% YoY growth) ¹¹⁷ [≫]. ¹¹⁸	Can only bulk load data from Amazon S3.

¹¹¹ For AWS see: Amazon Athena; Amazon Interactive Video Service; Amazon Kinensis Video Streams; Amazon Omics; Amazon Pinpoint; Amazon RedShift; Amazon SageMaker; Amazon SageMaker DataWrangler; Amazon Timestream; and AWS IoT Events Documentation. For Microsoft see: Azure Stream Analytics; and Azure IoT Hub.

¹¹² AWS' response to Ofcom's information requests [\gg].

¹¹³ 'Interactive Live Streams – Amazon Interactive Video Service – Amazon Web Services', accessed 23 May 2024.

¹¹⁴ AWS' response to Ofcom's information requests [>].

¹¹⁵ 'Genomic Data Analysis – Amazon Omics Customers – Amazon Web Services', accessed 23 May 2024.

¹¹⁶ AWS' response to Ofcom's information requests [\gg].

¹¹⁷ [>]. AWS' follow up response to Ofcom's information requests [>].

¹¹⁸ AWS' response to Ofcom's information requests [\gg].
Supplier	Service	Uptake	Potential limits to interoperability ¹¹¹
AWS	Amazon SageMaker	\$[≫] ([≫]% YoY growth) ¹¹⁹	Can only access training data from Amazon S3, Amazon EFS and Amazon FSx.
AWS	Amazon SageMaker Data Wrangler	This product is ancillary to Amazon SageMaker.	Can only import data from Amazon S3, Amazon Athena, Amazon Redshift, Snowflake, and Databricks.
AWS	Amazon Timestream	\$[≫] ([≫]% YoY growth) ¹²⁰	Can only use AWS' Backup service to manage backups.
AWS	AWS IoT Events	\$[≫] ([≫]% YoY growth) ¹²¹	Can only trigger actions with other AWS services.
Microsoft	Azure Stream Analytics	\$[⊁]([⊁]% YoY growth) ¹²²	Exclusively support native Azure services as inputs.
Microsoft	loT Hub	\$[≫] ([≫]% YoY growth) ¹²³	Allows basic interoperability but prioritises integration with other Azure service.

Source: Ofcom

AWS and Microsoft views

- 5.72 AWS disagreed with Ofcom's analysis of asymmetry of integrations. In its response to Ofcom's interim report, AWS said that Ofcom had only identified interoperability limitations in a small subset of its cloud services, focusing on ten services for which there are competing software solutions available that customers can run on AWS (or elsewhere). In addition, AWS said that the features identified as limiting interoperability are described inaccurately, exist alongside features that ensure interoperability, or are the product of an objective technical limitation.¹²⁴
- 5.73 Microsoft also disagreed with Ofcom's analysis of asymmetry of integrations. In its response to Ofcom's interim report, Microsoft said that temporary limitations of interoperability between first and third party cloud services are trade-offs in customer decisions to adopt multi-vendor or multi-cloud architectures. Microsoft attributed these limitations to the natural result of innovation from cloud providers which may take some time to be incorporated and enabled by ISVs or other cloud providers. In addition, Microsoft said that it does not have a strategy to frustrate interoperability and that it is not

¹¹⁹ Ofcom analysis of AWS' response to Ofcom's information requests [\approx].

¹²⁰ AWS' response to Ofcom's information requests [\gg].

 $^{^{121}}$ Ofcom analysis of AWS' response to Ofcom's information requests [\succ]. [\succ].

 $^{^{122}}$ Ofcom analysis of Microsoft response to Ofcom's information requests [\times].

¹²³ Ofcom analysis of Microsoft response to Ofcom's information requests [\times].

¹²⁴ AWS' response to Ofcom's Interim Report dated 5 April 2023, paragraphs 24-26.

accurate to characterise the services identified in the interim report as not interoperable.¹²⁵

Our initial assessment

- 5.74 We have carried out an initial review of Ofcom's list of AWS and Microsoft asymmetries of integrations. This is a preliminary analysis, and we are continuing to analyse the evidence.
- 5.75 Given their large market share, AWS and Microsoft appear most relevant; however, we are considering whether and how to include other cloud providers in this analysis.
- 5.76 Ofcom said that, during the market study, AWS made changes to Amazon SageMaker and SageMaker Data Wrangler, such that its users no longer experienced the limitation to interoperability that Ofcom had found in relation to these services.¹²⁶
- 5.77 Our initial review of relevant AWS publications,¹²⁷ suggests that these changes remain in place.
- 5.78 Microsoft told us that it recently enabled Azure Stream Analytics to support Apache Kafka input/output capability, which allows customers to configure non-Azure services as data sources directly and to interact with Azure Stream Analytics more easily from other applications, including those running on other clouds.¹²⁸
- 5.79 Our initial view is that allowing direct integration with a popular open-source data streaming software is sufficient to address the limitation to interoperability that Ofcom had identified in relation to this service.
- 5.80 We have identified a potential asymmetry of integrations with Azure Fabric, a service that allows enterprises to integrate their data across multiple clouds for the purposes of data analytics and AI. This asymmetry may be between different third party services rather than between first- and third party services: we have identified that Azure Fabric can export data to Azure Blob Storage and Amazon S3, but not directly to Google Cloud Storage.¹²⁹ We will

¹²⁵ Microsoft's response to Ofcom's Interim Report dated 5 April 2023, paragraphs 212-216.

¹²⁶ Ofcom Final Report dated 5 October 2023, paragraph 5.73 and A4.48-A4.52.

¹²⁷ See 'Use Snowflake as a data source to train ML models with Amazon SageMaker', accessed 23 May 2024.

¹²⁸ Microsoft's response to CMA's information request [>].

¹²⁹ See 'Data pipeline connectors in Microsoft Fabric - Microsoft Learn', accessed 23 May 2024.

investigate this potential asymmetry and would welcome any additional information on these potential differences.¹³⁰

- 5.81 We have also seen evidence of some instances of asymmetry of integrations relating to IAM which is an ancillary service or tool that allow customers to control who (person or application) can access what in the cloud.
- 5.82 In particular, a cloud provider said that Microsoft's IAM service Entra ID (formerly Azure Active Directory) allows third parties to 'tie into' it but this is not bi-directional. This means that it is possible to authenticate for that cloud provider's services using a Microsoft ID (ie @outlook domain), but it is not possible to use that cloud provider's domain to authenticate for Microsoft products.¹³¹

Other views

- 5.83 We asked customers about the potential impact of asymmetries of integration on their ability to integrate multiple clouds. Their views differed.
- 5.84 Some customers said that asymmetry of integrations had an impact on their ability to integrate multiple clouds.¹³² A few of these also said that asymmetry of integrations required additional technical effort, such as middleware or custom solutions, which in some cases may prevent them from doing so.¹³³
- 5.85 A customer said that where there are asymmetry of integrations this impacts its ability to integrate multiple clouds but cloud providers are generally actively working on the development of their integration capabilities.¹³⁴
- 5.86 Other customers said that asymmetry of integrations does not impact their ability to integrate multiple clouds.¹³⁵
- 5.87 We also asked customers about the potential impact of asymmetries of integration on their ability to switch clouds. Views on this were mixed amongst customers.¹³⁶ A customer said that it has not experienced any asymmetry of integrations but that it can in principle have an adverse impact on its ability to integrate multiple clouds and switch between clouds. In particular, it said that database migrations commonly include a transitional period with data spread

¹³⁰ We understand that it is possible to output data from Azure Fabric to a REST connector, which could connect to Google. However, this approach would require additional effort by the customer to configure as compared to the Azure Blob Storage connector.

¹³¹ [\times] response to CMA's information request [\times]; Note of meeting with [\times].

¹³² Responses to CMA's information requests [\times].

¹³³ Responses to CMA's information requests [>].

¹³⁴ [>] response to CMA's information request [>].

¹³⁵ Responses to CMA's information requests [\times].

¹³⁶ Responses to CMA's information requests [\times]; Note of meeting with [\times].

across multiple clouds and any asymmetry in integration of storage services would make it harder to query data in the same fashion and join it together. However, this customer also said that asymmetry of integrations is not the main factor impacting its ability to multi-cloud and switch.¹³⁷

- 5.88 We also heard from an ISV and two cloud providers on asymmetry of integrations. This evidence is mixed: one cloud provider agreed with Ofcom's analysis; the other considered that the issue raised competition concerns; the ISV suggested that cloud providers, such as AWS, are working to address the issue.
- 5.89 An ISV said that in some cases there may be a private API for a given service, or an integration must be done in a different way. It said that in some cases, for example with Microsoft, Google, and others, the provider has suggested that customers export data from the ISV's service into the cloud provider's own tool and the cloud provider 'takes it from there'. To illustrate the point, the ISV said that Amazon SageMaker normally requires data to be moved into an Amazon S3 bucket, and that this applied even for customers using data stored using other AWS services. It said that AWS provided a solution to this, but other cloud providers have not always been as 'productive'.¹³⁸
- 5.90 IBM submitted that a player with market power could reduce the functionalities of its products when used on third party cloud services, as opposed to when used on its own first-party cloud services. It said that when a provider exclusively provides (or significantly favours) cloud-related services within its own cloud infrastructure, this may affect competition, [≫]. IBM said that such conduct also reduces the customer's ability to choose between competing services and discourages the development of alternative solutions.¹³⁹
- 5.91 OVHcloud said it agrees with Ofcom's assessment of asymmetry of functionalities.¹⁴⁰

Our emerging views

5.92 We consider that asymmetries of integration may affect customers' ability to directly import, export and exchange data between cloud services and that customers may need to do so indirectly: they would need to use a different

¹³⁷ Note of meeting with [>].

¹³⁸ Note of meeting with [>].

¹³⁹ IBM's response to the Issues Statement, 17 October 2023, paragraph 1.6.

¹⁴⁰ OVHcloud's submission to CMA [>].

first-party service or a workaround, such as an adaptor which would incur additional cost.¹⁴¹

- 5.93 Our understanding is that, if a customer has to use an additional service or an adaptor that is offered by a third party as a managed service, this may include integration cost for setting up the service/adaptor and subscription cost for using it. If a customer is using its own adaptor, then this cost may be in the form of development cost, integration cost for setting it up, and operational cost for maintaining it, including ensuring that the adaptor works after each update of the first-party cloud service.¹⁴² We discuss the costs of using adaptors further in section 8 of this paper.
- 5.94 In addition, a temporary asymmetry of integrations may still disincentivise customers to integrate first- and third party services, if they expect a delay in being able to directly access the latest functionalities introduced by the hosting cloud.
- 5.95 The evidence we have seen to date suggests that there are core services with asymmetries of integrations.¹⁴³ These services have features that can be accessed when the service is directly integrated with another service by the same provider, but which cannot be accessed equally when using another provider, unless the customer uses another service by the same provider or a workaround.
- 5.96 The evidence is mixed on the impact of these asymmetries. It shows that for some customers asymmetry of integrations is a source of technical cost to multi-cloud and switching, although others have said this is not a challenge. We welcome additional evidence and views from stakeholders.
- 5.97 We welcome views on whether asymmetry of integrations is an area we should investigate further.

¹⁴¹ Workarounds, including adaptors, are further discussed in section 8 of this paper (Mitigation of technical costs to multi-cloud and switching).

¹⁴² Such updates may happen on a daily basis. For example, a customer said that AWS typically announces around 30-40 changes to their services every week ([\gg]).

¹⁴³ For example, we have seen evidence that these asymmetries exist in some services provided by AWS and Microsoft. On the basis of the evidence reviewed so far, we have not yet been able to determine the extent to which these asymmetries also exist in the services of other cloud providers.

6. Ancillary services and tools: evidence on sources of technical cost

- 6.1 In this section we consider whether there are technical costs incurred by customers when switching between and/or using multiple public clouds that arise from ancillary services and tools.¹⁴⁴ As discussed in section 3 of this paper, ancillary services and tools provide functions that support the operation and management of core cloud infrastructure services.
- 6.2 We begin by setting out evidence relevant to all ancillary services and tools (common themes) and we then set out evidence in relation to each main category of such services and tools: IAM, billing, observability, and provisioning and orchestration.
- 6.3 There are other categories of ancillary services and tools such as other security products (in addition to IAM), and software development and operations. We have not seen evidence to suggest that there are significant technical costs associated with these other areas. Nevertheless, we invite stakeholders to raise any concerns they may have with technical switching or multi-cloud costs related to other ancillary services and tools.

Common themes

6.4 Based on the evidence we have seen to date, we have identified some common themes that are relevant to all ancillary services and tools.

Potential mechanisms for impact on customers' ability to multi-cloud or switch

- 6.5 We understand that there are various mechanisms by which the design and implementation of ancillary services and tools can impact customers' ability to adopt a multi-cloud architecture or switch public cloud.
- 6.6 In general, differentiation of ancillary services and tools may add to the technical costs involved when integrating multiple public clouds or switching workloads between public clouds. For example, if the features or interfaces of ancillary services and tools are differentiated between public clouds, this may require customers to make additional changes to their applications, data and associated ancillary services and tools so that they can work and perform well on the target cloud. The scale of these challenges would likely vary by use-case and would usually depend on the number of applications that need to be

¹⁴⁴ In this section we discuss both IAM services, which are hosted by a supplier and typically accessed by a customer over the internet, and IAM software tools, which are installed and managed by the customer. Some IAM software tools are open-source software.

ported and the tightness of their integration into the proprietary services of the origin cloud.

- 6.7 We also consider that there are other ways in which ancillary services and tools may be associated with additional costs for customers who switch or integrate multiple public clouds. For example, the differentiation of core services (see section 5 of this paper) may cause customers who integrate multiple public clouds or switch public clouds to also expend resources redeveloping or reconfiguring the associated ancillary services and tools.
- 6.8 For clarity, in this section, by 'differentiation of ancillary services and tools' we mean differences (in features and/or interfaces) of comparable ancillary services and tools hosted on different public clouds and provided by any supplier, including cloud providers and ISVs.

Evidence from parties on the technical costs associated with ancillary services and tools

- 6.9 Some customers we spoke to said that the differentiation of ancillary services and tools has a negative impact on customers' ability to multi-cloud and/or switch. In particular, customers noted that the differentiation of ancillary services and tools increases the complexity and time in managing multiple clouds and switching between clouds.¹⁴⁵
- 6.10 For example, a customer said that replicating application functionality can be complicated by differences in the services of different cloud providers, requiring rework or mapping to different services to achieve the same goal. It also said that differences in APIs of ancillary services and tools require reworking of deployment pipelines, tooling or code.¹⁴⁶
- 6.11 Another customer said that the methods and philosophy behind ancillary services and tools are often completely different and it is hard to have one approach to multi-cloud. It said that each API is completely different meaning an entirely different software set-up is required. It also said that Infrastructure as Code and other software managing applications need to be re-written or adapted to work with another cloud.¹⁴⁷
- 6.12 Another customer said that each tooling 'jump' between suppliers of cloud services requires bridging a technical and conceptual gap, for example in

¹⁴⁵ Responses to CMA's information requests [>].

¹⁴⁶ [\times] response to CMA's information request [\times].

¹⁴⁷ [\gg] response to CMA's information request [\gg].

relation to different security frameworks and different systems of access control.¹⁴⁸

- 6.13 IBM said in relation to technical barriers that concerns may arise where there is a lack of portability of ancillary services and tools which are used once an application is running, eg to monitor performance, ensure security, compliance, logging, and metering. It said that a non-portable ancillary service or tool has to be recreated when using another cloud provider, which will involve additional technical work (mainly recoding) and may require different skillsets.¹⁴⁹
- 6.14 A supplier of professional services said that setting up and running multi-cloud is reasonably simple, but running it efficiently is quite complex and difficult. It said that for running an integrated multi-cloud architecture efficiently, a customer needs ancillary services and tools that cover all layers of their multi-cloud architecture, including infrastructure, network, APIs, applications and customer experience. This supplier said that, while the integration of such services is technically possible, it is also complex and requires specific skillsets and significant technical effort.¹⁵⁰
- 6.15 This supplier of professional services also said that ancillary services and tools differ significantly on how they perform their functions. For example, it said that ancillary services and tools produce different data in a different format and with different frequency.¹⁵¹
- 6.16 [**≻**]¹⁵²
- 6.17 However, some customers said that ancillary services and tools do not negatively impact their ability to multi-cloud and/or switch.¹⁵³ These customers did not elaborate on why this is the case.

Our emerging views

6.18 From the evidence we have reviewed to date, customers seem to experience challenges to multi-cloud and switching arising from ancillary services and tools in general, due to differences in both their features and their interfaces.

¹⁴⁸ Note of meeting with [>].

¹⁴⁹ IBM's response to the Issues Statement, 17 October 2023, page 3; and IBM's response to CMA's information request [%].

¹⁵⁰ Note of meeting with [\gg].

¹⁵¹ Note of meeting with [>].

¹⁵² [×]

¹⁵³ Responses to CMA's information requests [\gg].

Identity and access management

- 6.19 IAM refers to ancillary services and tools that allow customers to control who (person or application) can access what in the cloud. These services and tools perform two main functions authenticating identity and authorising access.¹⁵⁴ IAM is part of the broader category of security services and tools which aim to secure customers' cloud architectures.
- 6.20 We understand that for some purposes, customers who use the public cloud must use a cloud provider's own IAM service/tool.¹⁵⁵ In other cases, customers are able to choose additional functionality, services, or tools, for example in order to integrate multiple public clouds.¹⁵⁶

General impact of IAM on customers' ability to multi-cloud and switch

- 6.21 Many customers who we spoke to said that IAM is an important consideration and/or poses technical challenges when adopting a multi-cloud architecture or switching between clouds.¹⁵⁷ Most of these customers noted the differentiation of IAM across cloud providers as either the main reason or a significant reason for such technical challenges.¹⁵⁸
- 6.22 Consistent with this, a cloud provider said that technical differences between core IAM services from different clouds can significantly contribute to the challenge of using IAM services across clouds. It said that some of these differences may originate from the implementation of standards and protocols related to how identity information is managed and processed. It said that differences in the level of abstraction provided by IAM services, as well as the granularity of access supported can also be a factor. It also said differences in the ecosystem and related configurations can also result in adding complexity to the use of IAM services across clouds.¹⁵⁹
- 6.23 The Jigsaw report also found that providers' authentication methods are seen by customers to be different, which makes portability of IAM a particularly tricky topic.¹⁶⁰

- ¹⁵⁷ Responses to CMA's information requests [\gg]; Notes of meetings with [\gg].
- ¹⁵⁸ Responses to CMA's information requests [\times]; Notes of meetings with [\times].

¹⁵⁹ [>] response to CMA's information request [>].

¹⁵⁴ 'What is Cloud Identity and Access Management? – Pingldentity', accessed 2 May 2024.

¹⁵⁵ 'When do I use IAM? – AWS Documentation', accessed 25 April 2024.

¹⁵⁶ 'Okta Directory Integration – An Architecture Overview – Okta Resources', accessed 2 May 2024.

¹⁶⁰ Cloud Services Market Investigation Qualitative Customer Research conducted by Jigsaw (2024), paragraph 4.1.9 (b).

- 6.24 However, a few customers we spoke to suggested that IAM may not pose technical challenges for them when adopting a multi-cloud architecture.¹⁶¹
- 6.25 In addition, Oracle said that there are no significant feature differences between IAM services amongst cloud providers and that, in general, the major platforms all seem to support common industry standards.¹⁶²
- 6.26 In what follows, we have considered the evidence on the two key parts of IAM: identity authentication and access authorisation.

Impact of identity authentication on customers' ability to multi-cloud and switch

- 6.27 Some customers told us that they have integrated identity authentication functionality between multiple public clouds, by either 'federating' multiple cloud providers' individual IAM services or using a third party identity management service such as Okta.¹⁶³ We understand that customers do this in order to simplify the management of multiple public clouds, or for example to create a 'single sign-on' experience for customers' staff.¹⁶⁴
- 6.28 Some of these customers said they were able to integrate multiple cloud providers' IAM services across public clouds and did not experience significant technical challenges.¹⁶⁵
- 6.29 Other customers said they were able to integrate Microsoft Entra ID with other IAM services and this does not impact their choice of cloud provider for non-Microsoft related workloads.¹⁶⁶
- 6.30 Two cloud providers said that identity authorisation is harmonised across public clouds. Specifically, they said they use standard identity protocols (such as SCIM, SAML, and OICD¹⁶⁷), such that authentication can easily be performed by using third party identity providers:
- 6.31 AWS said that the authentication of users of all AWS services can be performed with third party identity providers such as Okta, through the Amazon Identity Center, which connects them via industry-standard protocols.

¹⁶¹ Responses to CMA's information requests [>].

¹⁶² Oracle's response to CMA's information request [\gg].

¹⁶³ Responses to CMA's information requests [\gg]; Note of meeting with [\gg].

¹⁶⁴ 'Microsoft Entra single sign-on (SSO) – Microsoft Security', accessed 2 May 2024.

¹⁶⁵ Responses to CMA's information requests [%]; Note of meeting with [%].

¹⁶⁶ Responses to CMA's information requests [\gg].

¹⁶⁷ We understand that Security Assertion Markup Language (SAML) and Open ID Connect (OIDC) are standard protocols that standardise the process of authenticating and authorising users when they sign in to access digital (and cloud) services. We understand that System for Cross-domain Identity Management (SCIM) is another standard protocol that enables the management of user accounts, groups, and some level of 'access' across different digital (and cloud) services.

It said that its support for industry-standard protocols, such as SCIM, SAML, and OIDC, eases customers' ability to store identities with an identity provider and then manage and use those identities with external applications.¹⁶⁸ AWS also said that Amazon Identity Center now offers seven tested SCIM integrations,¹⁶⁹ which we understand to be with CyberArk, Google Workspace, JumpCloud, Microsoft Entra ID, Okta, OneLogin, and Ping Identity products.¹⁷⁰

- 6.32 Oracle said it supports authentication via industry standards and provides tutorials for popular identity providers. It said that this allows customers to configure third party identity providers.¹⁷¹
- 6.33 Nevertheless, some customers noted technical challenges associated with the integration of identity authorisation functionality across clouds or switching suppliers.¹⁷²
- 6.34 For example, a customer said that it is possible to integrate Okta into multiple clouds, but the integration is complex because the integration efforts mostly sit with the customer and entail continuous work as integrations need to be applied to any new applications, services, workloads. This customer said that as a result, from an integration perspective, it may be simpler to use just one cloud but that is not necessarily the right choice.¹⁷³
- 6.35 Another customer said that cloud providers' products have different levels of portability based upon the degree of engineering effort required to integrate these products into applications and systems. For example, products such as storage services represent minimal challenges to portability whereas proprietary managed database services or identity management services represent greater complexity and thus effort to port to alternative vendors.¹⁷⁴
- 6.36 Three cloud providers also suggested that differences in identity authentication between public clouds remain.
- 6.37 A cloud provider said all major cloud providers provide the same level of interoperability with identity providers through standard identity protocols, such as OAuth, SAML and OIDC, making integration with third party IAM service easier. But it said that each cloud provider has its own nuances in the

 $^{^{\}rm 168}$ AWS, submission to CMA [\succ].

¹⁶⁹ AWS, submission to CMA [\geq].

¹⁷⁰ 'AWS IAM Center – Getting started tutorials', accessed on 25 April 2024.

¹⁷¹ Oracle's response to CMA's information request [\gg].

¹⁷² Responses to CMA's information requests [\times]; Notes of meetings with [\times].

¹⁷³ Note of meeting with [\geq].

¹⁷⁴ Note of meeting with [>].

implementations of these interoperable frameworks in terms of configuration and access mapping, which can impact consistency.¹⁷⁵

- 6.38 Another cloud provider said that Microsoft does not support inbound SCIM for Microsoft Entra ID. It said that as a result SCIM cannot be used to provision identities maintained primarily in another identity service (such as Okta) into Microsoft Entra ID. It also said that identity service providers must build custom integrations specific to Microsoft Entra ID, which are costlier to build and may not provide the same level of customer experience.¹⁷⁶ We understand that SCIM allows for the management of user accounts, groups, and some level of 'access' control, and is intended to make managing identities across difference cloud services easier.¹⁷⁷
- 6.39 Another cloud provider said that customers with a hybrid or multi-cloud architecture often find it challenging to access resources in one environment from a different environment. It said that customers can use Microsoft IDs to authenticate users of third party solutions, but generally cannot use a third party domain to authenticate users of Microsoft solutions. It said that this significantly increases management overheads from maintaining fragmented directories duplicated across different systems.¹⁷⁸

Impact of access authorisation on customers' ability to multi-cloud and switch

- 6.40 In relation to access authorisation, the other key IAM function, some customers we spoke to said that differences in access management can lead to additional technical costs for customers' who integrate multiple clouds or switch workloads between public clouds. In particular, they noted the need to translate and maintain access policies across clouds.¹⁷⁹ For example:
- 6.41 A customer said that it is experiencing increasing challenges in IAM, with individual cloud providers' PaaS offerings becoming tightly coupled with their IAM services. It said that while this simplifies managing business services operating on one cloud, it increases the effort to exit any provider because the access policies need to be translated and reproduced into another provider's context.¹⁸⁰
- 6.42 Another customer said that access management is a challenge in IAM. It gave the example of IAM policy scripts which it said are particularly important for security. In particular, it said that IAM policy scripts are currently not

¹⁷⁵ [>] response to CMA's information request [>].

¹⁷⁶ [\gg] response to CMA's information request [\gg].

¹⁷⁷ 'SCIM: System for Cross-domain Identity Management', accessed 26 April 2024.

¹⁷⁸ [>] response to CMA's information request [>].

¹⁷⁹ Responses to CMA's information requests [%]; Notes of meetings with [%].

¹⁸⁰ [>] response to CMA's information request [>].

standardised between public clouds (eg and Azure) and require deep knowledge, which is not transferable between public clouds.¹⁸¹

- 6.43 A cloud provider gave IAM as an example of technical difficulty which it or its customers can encounter when seeking to integrate its services with those of other public clouds. In particular, this cloud provider said that authorisation policies and access controls are cloud-specific and concepts used by one cloud provider may not have exact translations in another public cloud. For example, it said that different cloud providers may represent users in different ways or as different/multiple entities. The cloud provider also said these differences may contribute to difficulty for customers, but that depends on factors including how familiar or comfortable users are with one cloud provider's resources and authorisation policies versus another cloud provider's. It said that customers will likely find the options that cause them the least amount of work and/or rework to implement and/or maintain cross-cloud solutions.¹⁸²
- 6.44 Another cloud provider, IBM, mentioned that there are technical challenges in relation to access authorisation. It said that there are some known differences in how access policies are defined, their structure, as well as conditions attached to them, such as those relating to time-based access or network location access.¹⁸³
- 6.45 An ISV said that access management in general lacks the same level of industry standards as identity management. However, it said that, in its view, AWS is working to solve this through the open-source Cedar Policy Language and that there may be other options.¹⁸⁴

Microsoft's IAM software and services

6.46 We heard two concerns specifically about Microsoft's IAM services and tools, which we understand could present technical challenges for Microsoft customers when switching or integrating multiple public clouds.

Technical challenges with Active Directory

6.47 The first concern relates to Microsoft Active Directory, which is IAM software that is commonly used in customers' on-premises IT set ups. A cloud provider said that Microsoft does not support modern protocols such as SAML and OIDC in Active Directory, and does not provide sufficient access to Active

¹⁸¹ Note of meeting with [>].

¹⁸² [\times] response to CMA's information request [\times].

¹⁸³ IBM's response to CMA's information request [\times].

¹⁸⁴ [\gg] response to CMA's information request [\gg].

Directory's APIs or technical information,¹⁸⁵ which it said makes it very challenging for users to integrate Active Directory with IAM services and tools other than Microsoft's cloud IAM service, Entra ID. It said that Entra ID is entirely interoperable with Active Directory,¹⁸⁶ and as a result, most customers with Microsoft-related workloads continue using their on-premises Active Directory with Entra ID. This cloud provider also said that this technical challenge, together with licensing conditions,¹⁸⁷ make it uneconomical for customers to switch Microsoft-related workloads to other cloud providers.¹⁸⁸

- 6.48 Some customers said that they selected Entra ID based on their use of Active Directory.
- 6.49 A customer said that it has tended towards using Entra ID (Azure Active Directory), which is a technical decision based on its established Active Directory footprint, because it supports the most secure industry standard password-less authentication protocols needed for its multi-cloud strategy, and it does not force it to use Microsoft's services for cloud computing or storage.¹⁸⁹
- 6.50 A customer said that Microsoft's integration with its traditional components makes Office 365 and Entra ID unviable to deviate from.¹⁹⁰
- 6.51 A customer said that in the longer term it expects to retire Active Directory and move entirely to a cloud only IAM solution, which is likely to be Entra ID.¹⁹¹
- 6.52 We will consider further the extent to which customers who use Active Directory are able to switch associated workloads between cloud providers, and in particular, whether such customers are able to switch these workloads to, or develop related workloads in, public clouds other than Azure.

Using Entra ID with other Microsoft software and services

6.53 We have also heard that customers who use other Microsoft software and services may be incentivised to use Entra ID over competing IAM services to manage their public cloud, and that this could affect those customers' decision-making in relation to switching and/or integrating multiple clouds.

¹⁸⁵ [>] response to CMA's information request [>].

¹⁸⁶ [>] response to CMA's information request [>].

¹⁸⁷ Licensing conditions will be discussed further in a separate working paper.

¹⁸⁸ [\gg] response to CMA's information request [\gg].

¹⁸⁹ [\times] response to CMA's information request [\times].

¹⁹⁰ [\gg] response to CMA's information request [\gg].

¹⁹¹ [\times] response to CMA's information request [\times].

- 6.54 A cloud provider said that Microsoft offers Entra ID (Azure Active Directory) for free to customers who purchase software licences for Microsoft 365, despite these being separate products.¹⁹²
- 6.55 A customer said that due to the integration of Entra ID with Microsoft 365 and other Microsoft security products, and the breadth of capability this integration then offers, it is unlikely to switch away from Entra ID in the short to medium term.¹⁹³
- 6.56 CFSL and another organisation suggested that there is a requirement to use Microsoft's IAM service Entra ID) to manage other Microsoft software, and that in particular this represents a barrier for customers who use Microsoft 365 on other providers' clouds.¹⁹⁴
- 6.57 A cloud provider said that Microsoft requires customers to use Entra ID to 'provision/authenticate' Microsoft 365 subscriptions/users. It said that this is required even if the customer already uses a separate third party identity solution.¹⁹⁵
- 6.58 An industry body said that Microsoft does not disclose the interoperability information, nor provide any APIs needed, to allow interoperability between Entra ID and third party identity management products.¹⁹⁶
- 6.59 We invite views from stakeholders on the extent to which customers who use other Microsoft products are able to choose IAM services other than Entra ID, and the extent to which using Entra ID impacts customers' ability to switch related workloads between clouds. We also invite views on whether access to technical interoperability information on Microsoft's IAM services and tools would help customers switch related workloads between clouds.

Our emerging views

- 6.60 The evidence we have seen to date shows that there may be significant technical costs associated with IAM for customers who integrate multiple public clouds or switch public clouds.
- 6.61 This evidence also indicates that the extent of this technical cost seems to vary depending on the specific function that the IAM service or tool is being used for. In particular, there may be variation between identity authentication and access management. It seems that costs associated with integrating

¹⁹² [\gg] response to CMA's information request [\gg].

¹⁹³ [>] response to CMA's information request [>].

¹⁹⁴ [\times] submission to CMA [\times]; and CFSL's response to the Issues Statement, 17 October 2023, pages 19-21.

¹⁹⁵ [\times] response to CMA's information request [\times].

¹⁹⁶ [\succ] submission to CMA [\succ].

identity authentication across multiple public clouds appear to be lower, potentially due to the adoption of standard identity protocols. Conversely, there appear to be significantly higher costs for customers who switch public clouds or integrate multiple public clouds and have to rewrite or synchronise access policies and configuration.

Billing

6.62 Billing refers to ancillary services and tools that monitor and analyse the financial cost of provisioned cloud services in real time. These services and tools help customers monitor usage costs, forecast spending, and identify opportunities for savings. Billing services and tools are fundamental for any customer and any cloud use.

Impact of billing on customers' ability to multi-cloud and switch

- 6.63 A customer said that cloud billing is 'painful and difficult to work with'. It said a lack of standardisation on what different fields mean in its bills makes comparing bills difficult across cloud providers. This customer said it had to develop an expensive workaround, including an in-house tool to make billing data comparable across clouds and present it in a central dashboard.¹⁹⁷
- 6.64 However, some customers said that billing services and tools have facilitated their use of multi-cloud. In particular, these customers said they use cloud-agnostic billing services and tools offered by ISVs, such as Apptio Cloudability and VMware CloudHealth, to aggregate and analyse bills across the public clouds they are using.¹⁹⁸ One of these customers said that these services and tools have grown in popularity with the economic changes like rising costs, inflation, and global market volatility.¹⁹⁹
- 6.65 We also understand that Microsoft provides pre-built integrations and AWS provides documentation that help customers use their first-party billing services to view billing information from each other's public clouds:
- 6.66 Microsoft provides an integration that allows customers to monitor and control their AWS spending from within the Azure Cost Management billing service.²⁰⁰ However, we understand that Microsoft intends to retire this integration in March 2025.²⁰¹

¹⁹⁷ Note of meeting with [>].

¹⁹⁸ Responses to CMA's information requests [%]; Notes of meetings with [%].

¹⁹⁹ Note of meeting with [>].

²⁰⁰ 'Set up and configure AWS Cost and Usage report integration – Microsoft Learn', accessed 26 April 2024.

²⁰¹ 'Retire your AWS connector – Microsoft Learn', accessed 26 April 2024.

6.67 AWS does not appear to provide a similar integration but has published documentation that explains how to set up a similar solution, in which Azure cost data and reports can be monitored using the AWS QuickSight billing service.²⁰²

Our emerging views

6.68 Based on the evidence we have reviewed to date, our emerging view is that, while billing services and tools may be associated with technical challenges to customers' ability to multi-cloud or switch, the impact of such challenges may be low, at least for some customers. This is because some customers do seem to be able to effectively adopt cloud-agnostic billing services and tools, which we understand makes it easier to manage billing across multiple public clouds, and therefore may reduce the associated technical costs. We welcome views from stakeholders on the impact that billing services and tools have on customers' ability to integrate multiple public clouds or switch between clouds.

Observability

6.69 Observability refers to ancillary services and tools that measure, analyse and visualise the current state of a customer's cloud architectures based on the data it generates, such as logs, metrics, and traces. This allows customers to determine the health of an application, workload, or system, so they can act to secure and maintain performance and availability.²⁰³

Impact of observability on customers' ability to multi-cloud and switch

- 6.70 We understand that there are some industry efforts to standardise observability across clouds. In particular, OpenTelemetry seems to be gaining popularity with suppliers and customers.²⁰⁴
- 6.71 We understand that OpenTelemetry consists of both formal specifications and open-source software packages and if a customer adopts a cloud architecture based on OpenTelemetry then it is easier for them to switch observability tools as they switch or integrate multiple public clouds.²⁰⁵
- 6.72 Many observability services and tools appear to support OpenTelemetry, meaning they are designed to be compatible with OpenTelemetry

²⁰² 'How to view Azure costs using Amazon QuickSight – AWS Blog', accessed 26 April 2024.

²⁰³ 'CNCF Observability Micro Survey: Cloud Native Observability: hurdles remain to understanding the health of systems', accessed 26 April 2024.

²⁰⁴ 'OpenTelemetry announces support for profiling – CNCF blog', accessed 26 April 2024.

²⁰⁵ 'What is OpenTelemetry? – OpenTelemetry Documentation', accessed 26 April 2024.

specifications and software packages. This includes services and tools offered by AWS, Microsoft, Google, Oracle, and IBM.²⁰⁶

- 6.73 Some customers told us that they have a preference for services and tools that support OpenTelemetry.²⁰⁷ This includes a customer that said it is moving to OpenTelemetry as its monitoring solution because, in its view, its current solution could be improved and there will be a lot of competition in this field over the next two years.²⁰⁸
- 6.74 An industry body said that observability is an area which could benefit from some standardisation because the outputs and functions of comparable services are sufficiently similar.²⁰⁹
- 6.75 There are also efforts to increase standardisation in other parts of the observability stack, although these efforts seem to be at an early stage. In particular, OpenMetrics is a newly developed open standard for metrics and there is ongoing work to develop a standardised query language for observability data.²¹⁰
- 6.76 We have also seen evidence of other efforts that cloud providers put to improve observability. In particular, Oracle said that its monitoring APIs may be used by third parties to create their own monitoring services. It said that its Grafana plug-in allows customers to use OCI as a data source for Grafana.²¹¹
- 6.77 However, some customers said that observability services and tools give rise to technical challenges to multi-cloud and to a lesser extent switching.²¹²
- 6.78 For example, a customer said that, while there are standards like OpenTelemetry at the lower end of the observability stack, the ecosystem remains fragmented at the higher end of the stack. It said observability across multiple clouds is difficult. It also said that it has switched observability suppliers several times and that there are technical challenges in doing this.²¹³
- 6.79 Another customer said that in relation to multi-cloud that visibility of services that have been built or migrated is probably the hardest thing to deliver. It said that new tools and processes are required, which often means increased

²⁰⁶ 'Vendors – OpenTelemetry Documentation', accessed 26 April 2024.

²⁰⁷ Note of meeting with [>].

²⁰⁸ Note of meeting with [>].

²⁰⁹ Note of meeting with [>].

²¹⁰ 'Query Standardization Working Group – CNCF Technical Advisory Group for Observability GitHub repository', accessed 26 April 2024 and 'OpenMetrics (a CNCF sandbox project)', accessed 26 April 2024.

 $^{^{211}}$ [%] response to CMA's information request [%].

²¹² [\times] response to CMA's information request [\times]; Notes of meetings with [\times].

²¹³ Notes of meetings with [>].

costs and uplift in skills to support. This customer said in relation to switching that its biggest barrier is the tooling and telemetry, which is usually tied to the specific cloud. It said that any migration to another hosting provider would not only need re-engineering of the application/platform, but all of the security and observability required for the service.²¹⁴

Our emerging views

6.80 From the evidence we have seen to date, there appears to be some impact on customers' ability to switch public cloud or integrate multiple public clouds arising from observability services and tools. While the development and adoption of OpenTelemetry may improve interoperability, it does not seem to eliminate the issues in all cases.

Provisioning and orchestration

- 6.81 Provisioning and orchestration refers to ancillary services and tools that automate the tasks needed to manage deployment, connections and operations of workloads. These include Infrastructure as Code (IaC) services and tools and container orchestration services and tools.
- 6.82 For example, we understand that each cloud provider offers a proprietary IaC service that allows cloud engineers to formally specify their cloud architectures and the cloud infrastructure services that they use.²¹⁵ Using these services helps cloud engineers automate processes that they would need to otherwise manage manually, and in general simplify the management of complex workloads in the public cloud.²¹⁶
- 6.83 We also understand that some cloud providers offer proprietary container management cloud infrastructure services, some of which integrate natively with other services available on those provider's clouds.²¹⁷ We understand that some of these services are managed services of open-source software, such as Kubernetes,²¹⁸ (an open source, cloud-agnostic container orchestration platform) and can significantly reduce the management costs associated with using containers.²¹⁹
- 6.84 We understand that, in relation to provisioning and orchestration services and tools, there are differences between cloud providers' own services and

²¹⁶ 'What is Infrastructure as Code Iac)? – Red Hat documentation', accessed 8 May 2024.

²¹⁸ 'Amazon EKS – AWS Documentation', accessed 13 May 2024.

²¹⁴ [\gg] response to CMA's information request [\gg].

²¹⁵ ¹IaC tools comparison shows benefits of automated deployments - TechTarget', accessed 8 May 2024.

²¹⁷ Menga, J (2018), Docker on Amazon Web Services, Packt Publishing Ltd, page 21.

²¹⁹ 'Choosing an AWS container service', accessed 10 May 2024.

tools,²²⁰ but that cloud-agnostic tools, such as Terraform and Kubernetes, can also be used. AWS told us that open-source software such as Terraform and Kubernetes is gaining in popularity.²²¹

- 6.85 We have heard that using cloud-agnostic services and tools can therefore mitigate costs involved with switching or multi-cloud.²²² We discuss these mitigations in more detail in section 8 of this paper.
- 6.86 We have not seen any evidence from customers that differences between provisioning or orchestration services and tools are currently a significant source of technical multi-cloud and switching costs.

Our emerging views

- 6.87 Based on the evidence reviewed to date, provisioning and orchestration services and tools do not appear to pose significant technical challenges to customers' ability to multi-cloud or switch.
- 6.88 We note that there are established open-source tools in this area, such as Terraform and Kubernetes, which may simplify the management of provisioning when using multi-cloud or when switching. We welcome further views on the extent to which provisioning and orchestration remain a challenge to customers when switching or using multi-cloud.

²²⁰ 'Infrastructure as Code IaC): Comparing the Tools – Microsoft ITOps Talk Blog', accessed 8 May 2024. ²²¹ AWS' submission to CMA [\approx].

²²² [\times] submission to CMA [\times]; and Cloud Services Market Investigation Qualitative Customer Research conducted by Jigsaw (2024), page 58.

7. Other technical factors: evidence on sources of technical cost

7.1 In this section we consider other technical factors which could increase the costs associated with integrating public clouds or switching between public clouds, specifically data latency, skills and transparency. These factors may arise separately from the purely technical details of core and ancillary service design, but nevertheless can have implications on the ability of customers to integrate between clouds and switch.

Latency

- 7.2 Latency refers to the time it takes for data to travel between any two points on a network. In relation to public cloud, this could be the time it takes for data to move within a single data centre, between the data centres of the same public cloud, between different public clouds or between the public cloud and other IT environments. It could be the time it takes for data to move between two parts of the customer's cloud architecture or between the customer and a third party such as a partner or a client of the customer.
- 7.3 Latency is bound by the speed of light. This means that latency is generally lower when data is travelling over short distances and higher when it travels long distances.²²³ As such, latency is lower when data is travelling within the same data centre, higher when travelling between data centres located in the same geographic area (eg in the same availability zone²²⁴) and higher still when travelling between geographic areas (eg between regions).
- 7.4 Latency is also determined by the speed of processing at any interim nodes on the path of data transfer. This means that latency is lower when data is travelling directly between the origin and target points of the network and higher when it must pass through various nodes that process the data between these points. The data centres of cloud providers can be connected directly or indirectly depending on how closely they are located and whether they are part of the same public cloud.
- 7.5 The data centres of the same public cloud within the same geographic area, which some providers call 'availability zones', may be connected directly with a fibre line. This scenario has relatively low latency because there are no

²²³ 'What is Network Latency? – AWS documentation', accessed 9 May 2024.

²²⁴ An Availability Zone (AZ) is a collection of one or more data centres on which public cloud services operate. AZs are grouped within geographic regions to enable low latency connections between data centres but are sufficiently isolated such that events like natural disasters and power outages should not impact service provision across the entire AZ.

interim nodes on the network and the data must traverse only a small distance. We understand that AWS, Microsoft and Google offer low latency connections for internal data transfers within availability zones.²²⁵ Other cloud providers may have similar approaches.

- 7.6 The data centres of the same public cloud in different geographic regions rely on the cloud providers' own 'backbone' network infrastructure which consists of physical hardware such as routers and fibre cables. Whilst data travelling between two data centres in different regions on the same cloud platform will generally not use the public internet, this scenario does still entail higher latency because data will not necessarily be transferred directly between the two data centres and must travel longer distances.²²⁶
- 7.7 The data centres of different public clouds are generally connected using the public internet. In this scenario, latency is higher still because data must travel through one or more Internet Exchange Points (IXPs). These act as interim nodes on the network which means data transfer is slower in comparison to a more direct connections between two locations. We understand that there are services such as Amazon Direct Connect, Azure Express Route and Google Dedicated Interconnect which allow customers to connect different clouds more directly.²²⁷ This architecture entails some configuration effort by the customer. Some services such as Google Cross Cloud Interconnect aim to offer similar connections but without requiring management by customers.²²⁸ We invite views on the use of methods which allow direct connections between clouds, for example how commonly they are used and the complexity involved.
- 7.8 We heard from a few customers that latency requirements mean that applications perform more strongly when they are located on a single cloud platform, particularly when they are processing real-time data.²²⁹ For example, a customer said that transferring data between clouds introduces the risk of latency, which can affect application performance; it generally recommends internally to keep technologies to a single provider to prevent this.²³⁰
- 7.9 The Jigsaw report is consistent with this, finding that customers who need to process or transmit data in real time see latency as an inherent barrier to multi-cloud because it will likely decrease the speed of their applications and

²²⁵ 'Regions and Availability Zones', accessed on 19 April 2024; 'Azure Availability Zones', accessed on 19 April 2024; 'Google Cloud Networking Overview', accessed on 19 April 2024.

²²⁶ 'AWS Connectivity', accessed on 19 April 2024.

²²⁷ 'Designing Private Network Connectivity Between AWS and Microsoft Azure', accessed on 19 April 2024; 'Dedicated Interconnect Overview', accessed on 23 May 2024.

²²⁸ 'Cross Cloud Interconnect Overview', accessed on 19 April 2024

²³⁰ [\times] response to CMA's information request [\times].

workloads. It is therefore more logical to keep such workloads on a single cloud provider.²³¹

- 7.10 A few ISVs agreed with this, saying that latency can be an obstacle to multicloud because it can impact the performance and functionality of customers' applications.²³²
- 7.11 In contrast, some customers indicated that latency is not a significant concern to them.²³³ However, evidence suggests that this could be due to the nature of the data that is being processed. For example, a customer said that latency has a relatively low impact on its ability to integrate between clouds, because some of its workloads transfer data asynchronously, so the time taken for data to pass between public clouds is less important.²³⁴
- 7.12 There is conflicting evidence on the importance of latency for switching between public clouds. A few customers said it can be important, for example during the intermediate step where applications are duplicated between clouds.²³⁵
- 7.13 However, we also heard that latency may not be a barrier to switching. For example, a customer said that it previously moved some of its latency sensitive workloads but for a time carried on using the database stored in the previous cloud provider in the same region. The customer explained that connectivity was fast and did not cause any issues; it could even have maintained this architecture for an extended period.²³⁶
- 7.14 Separately, we have heard evidence that having a wide geographic dispersal of data centres can be important for customers because it may enable lower latency between their workloads and end users, such as customers and factories. For example:
- 7.15 A customer said that larger providers are more attractive than smaller providers because they have a greater number of data centres, meaning there is likely a smaller distance between its edge locations and the data centres to which they are connected. This is particularly important for some of its workloads which are latency-sensitive, such as the real-time control of robots.²³⁷

²³¹ Cloud Services Market Investigation Qualitative Customer Research conducted by Jigsaw (2024), paragraph 4.1.15.

²³² Notes of meetings with [>].

²³³ Responses to CMA's information requests [\gg].

²³⁴ Note of meeting with [>].

 $^{^{235}}$ Responses to CMA's information requests [\gg].

²³⁶ Note of meeting with [\gg].

²³⁷ Note of meeting with [>].

- 7.16 Similarly, another customer said that it sometimes uses multiple public clouds within a single workload because it requires data centres that are closer to the end users to reduce latency.²³⁸
- 7.17 The Jigsaw report highlighted that, in some sectors, data latency can influence initial vendor choice, particularly where there is a 'network effect'. This is where, due to considerations around data transfer speeds, a customer may be more inclined to utilise a cloud provider which is most commonly used among its suppliers or clients.²³⁹
- 7.18 Some cloud providers have told us that increased cost and reduced performance (eg higher latency) can be an unavoidable reality when attempting to integrate between cloud platforms which may discourage customers from integrating a single workload across multiple clouds.²⁴⁰ For example, AWS said that when a single solution is spread between multiple cloud providers, information may need to flow many hundreds of miles across the internet to move between services. This increases latency and cost due to the additional time it takes to transfer data between cloud providers.²⁴¹

Our emerging views

- 7.19 Based on the evidence we have seen to date, our emerging view is that latency can be a challenge to customers in integrating multiple public clouds when the integration involves workloads that require real-time or near-realtime transfers of data.
- 7.20 Latency requirements may also motivate customers to utilise multiple clouds where it enables them to reduce the geographic distance, and therefore time, between their workloads placed in data centres and end users.
- 7.21 We consider that latency remains an inherent feature of cloud infrastructure which may constrain customers' ability to integrate between and switch public clouds. There are some ways to mitigate issues posed by latency, discussed in section 8 of this paper.

Skills

7.22 To effectively manage its cloud architecture, an organisation will have employees who are skilled and experienced in cloud engineering. This

²³⁸ Note of meeting with [>].

²³⁹ Cloud Services Market Investigation Qualitative Customer Research conducted by Jigsaw (2024), paragraph 4.1.16.

²⁴⁰ Microsoft's response to the Issues Statement, 17 October 2023, paragraph 34; Responses to CMA's information requests [×].

²⁴¹ AWS' response to CMA's information request [\gg].

discipline is highly technical and the pace of innovation in the public cloud means that organisations must employ skilled professionals and train their existing workforce to optimise their environments.

- 7.23 The level of differentiation between the various public clouds will affect the extent to which skills may be a challenge which increases the cost of integrating clouds or switching between clouds.
- 7.24 Lack of skills may also be exacerbated by the other technical challenges discussed in sections 5 and 6 of this paper. In theory, any differentiation of interface that exists between two platforms requires the skillsets to work around this. There may also be some degree of circularity to this; an organisation unable to find workers sufficiently skilled to overcome the differentiation of interfaces problem will see this as a more significant factor.
- 7.25 We heard differing views on the extent to which skills are transferable between public clouds and the ease of retraining staff to work on alternative cloud platforms.
- 7.26 Some customers said that the skillsets required to operate on different providers are distinct and that the expense of retraining staff increases costs associated with multi-cloud and switching.²⁴² For example, a customer said that cloud skills are not uniform or universal across different providers, as each has its own tools, frameworks, methodologies and best practices that require specific knowledge and training. Therefore, switching between providers would entail a continuous investment in learning and developing the relevant skills and competencies for each provider.²⁴³
- 7.27 Some customers said that they make decisions related to their cloud architecture based, at least in part, on the skillsets that are already present in their organisations.²⁴⁴ For example, a customer said that some data analytics workloads are hard to move even though there is a strategically preferred offering from another provider. The customer explained that this is because its staff have developed knowledge of its current provider's data analytics technologies but not of other clouds' analogous services.²⁴⁵
- 7.28 We also heard from some customers that the differentiation in skillsets required for each cloud necessitates separate teams for each; the cost of this can be prohibitive to a multi-cloud architecture.²⁴⁶ For example, a customer said that one of its business units originally operated on two clouds, but it is in

²⁴⁵ Note of meeting with [>].

²⁴² Responses to CMA's information requests [\gg].

²⁴³ [>] response to CMA's information request [>].

²⁴⁴ Responses to CMA's information requests [\times]; Note of meeting with [\times].

²⁴⁶ [\times] response to CMA's information request [\times]; Notes of meetings with [\times].

the process of switching to one. The main reason for this is to reduce the complexity and overhead costs; the business does not want to maintain staff that are able to use both clouds.²⁴⁷

- 7.29 Another point we heard from a few customers is that the differentiation of skillsets required to operate different cloud platforms can lead to recruitment difficulties.²⁴⁸ For example, a customer said that it finds it hard to source engineers who are skilled in multiple clouds platforms because each has different philosophies, APIs and technical implementations.²⁴⁹
- 7.30 The Jigsaw report also indicated that customers find that shortages of skills in their existing workforce, as well as a difficult hiring environment can increase the costs of integrating and switching between cloud providers. The research further highlighted that most cloud engineers are expert in only one cloud provider, which necessitates expensive training or hiring new teams if seeking to integrate between or switch clouds. Even rarer than those with experience in multiple clouds, are engineers with experience of networking multiple clouds together, which is particularly important for an organisation's architectural security.²⁵⁰
- 7.31 The Jigsaw report also found that the human knowledge that a customer builds with a specific cloud provider over several years may be seen as a 'stranded asset' which can particularly impede switching. For example, customers may spend significant time and money developing knowledge of one provider, substantial amounts of which will be lost if the organisation moves to a different cloud provider. This can make such decisions difficult to justify, especially for larger customers with complex systems and architectures.²⁵¹
- 7.32 A supplier of professional services also said that skills can be a problem when switching. Companies are hesitant to train staff on multiple clouds due to cost and the competitive labour market for staff skilled in multiple clouds.²⁵²
- 7.33 An industry body said that there is now a large ecosystem of tools which are needed for developing applications and these tools are often unique to individual clouds. Its concern is less about mobility in the cloud, rather the

²⁴⁷ Note of meeting with [>].

²⁴⁸ Responses to CMA's information requests [\gg].

²⁴⁹ [\gg] response to CMA's information request [\gg].

²⁵⁰ Cloud Services Market Investigation Qualitative Customer Research conducted by Jigsaw (2024), paragraph 4.3.7.

²⁵¹ Cloud Services Market Investigation Qualitative Customer Research conducted by Jigsaw (2024), paragraph 4.3.5.

²⁵² Note of meeting with [>].

lock-in of developers to clouds, through the cost and time of retraining on these tools.²⁵³

- 7.34 In contrast, some customers said that they have found it relatively easy to retrain staff in other cloud providers' services, or that the skills they have are transferable between providers.²⁵⁴ For example, a customer said that cloud specific skills are not an important factor when choosing a provider because staff can be retrained and skills are transferable across clouds.²⁵⁵
- 7.35 An ISV also said it did not find it difficult to train its staff to operate across providers. It added however, that software engineers would have to learn some concepts around fault isolation and operations when learning how to work with a new provider and that this was akin to learning a new syntax.²⁵⁶
- 7.36 Furthermore, AWS said that moving data and changing services naturally takes some time and resources, which may require retraining of staff.²⁵⁷ Microsoft said that cloud providers invest heavily in innovation which brings inevitable complexity and leads to differentiation between the competing providers.²⁵⁸
- 7.37 Separately, two small cloud providers, said that the training programmes offered by larger providers can impact the wider cloud engineering labour market.²⁵⁹
- 7.38 One small cloud provider said that large providers, through comprehensive training and certifications, deeply influence students and professionals, swaying their cloud preferences from an early stage. Aggressive outreach can create a tech ecosystem where new talent is predominantly trained and biased towards a single cloud vendor, limiting multi-cloud knowledge, and curbing future diversification.²⁶⁰
- 7.39 Another small cloud provider said that it has become common for end users to recruit engineers with certifications from AWS, Microsoft & Google, rather than looking for those with the technical skills but no certification. This incites individuals to specialise in the services of these providers at the expense of those providers which are unable to offer formal certifications and training.

²⁵³ Note of meeting with [>].

²⁵⁴ Responses to ČMA's information requests [>>].

 $^{^{255}}$ [>] response to CMA's information request [>].

²⁵⁶ Note of meeting with [>].

²⁵⁷ AWS' response to the Issues Statement,17 October 2023, paragraph 21.

²⁵⁸ Microsoft's response to the Issues Statement, 17 October 2023, paragraph 23.

²⁵⁹ Cloud provider 1's response to the Issues Statement, 17 October 2023, section 3; [\times] response to CMA's information request [\times].

²⁶⁰ Cloud provider 1's response to the Issues Statement, 17 October 2023, section 3.

The provider also said that such training and retraining is offered to prevent clients from switching.²⁶¹

- 7.40 However, some large cloud providers said that the training they provide helps IT professionals to upskill and transfer their skillsets across clouds.²⁶² AWS said that skills are generally transferable between clouds and that there are many free and paid options for users to develop their skills with different providers.²⁶³ It also said that it offers training programmes to help customers achieve desired migration outcomes.²⁶⁴
- 7.41 We heard from some customers that the training offered by large cloud providers is an important consideration and can be an enabler of multicloud.²⁶⁵ For example, a customer said that the training offerings from providers have been an active enabler to multi-cloud.²⁶⁶ It said that it is not difficult to upskill on new platforms because providers are keen to help developers learn how to use their services.²⁶⁷

Our emerging views

- 7.42 Based on the evidence we have seen to date, our emerging view is that the need for cloud-specific skills amongst employees can increase costs for some, though not all, customers when seeking to integrate public clouds or switch between public clouds.
- 7.43 Although some customers report being able to train employees easily on new clouds, many others say that it is difficult, and that having to hire additional employees with different skillsets serves as a disincentive to multi-cloud and switching, especially as these required skillsets appear to be in relatively short supply. The extent to which customers are impacted by skills differentiation does not appear to be dependent on the size of their organisations.
- 7.44 Furthermore, whilst some customers explained that the training offered by large cloud providers is helpful for upskilling their employees, some smaller cloud providers said that it is potentially creating a prevalence of the skillsets required to operate on the larger platforms. This can be a factor relevant to customers' choices when considering the use of alternative public clouds for which the required skillsets are in relatively lower supply.

²⁶¹ [>] submission to CMA [>].

 $^{^{262}}$ AWS' response to the Issues Statement, 17 October 2023, paragraph 20; Responses to CMA's information requests [\gg].

²⁶³ AWS' response to the Issues Statement,17 October 2023, paragraph 20.

 $^{^{264}}$ AWS' response to CMA's information request [\gg].

 $^{^{265}}$ Responses to CMA's information requests [\gg].

²⁶⁶ [>] response to CMA's information request [>].

²⁶⁷ Note of meeting with [>].

Transparency

- 7.45 We considered whether cloud providers make available and discoverable sufficient technical information that could help customers overcome technical challenges when switching public clouds or integrating multiple public clouds. We understand that improving transparency about the interoperability of cloud infrastructure services could provide short-term benefits by facilitating switching, preventing lock-in and improving the viability of multi-cloud approaches.²⁶⁸ Greater transparency could also allow ISVs to develop cloud-agnostic services more easily, potentially enabling more multi-cloud and switching for their users.
- 7.46 Conversely, an insufficient degree of transparency may lead to customers expending undue effort when seeking to integrate or switch workloads or could hinder competition by dissuading users from exploring alternative cloud options. For example, we have seen evidence that updates and changes that cloud providers make to cloud infrastructure services may create confusion for customers.²⁶⁹
- 7.47 We heard differing views on the availability and discoverability of information about potential technical challenges, and whether this impacts customers' ability to switch public cloud or integrate multiple public clouds. Some said that it can impede their ability to switch;²⁷⁰ others said that it does not.²⁷¹ Separately, a few customers said that it can impact their ability to integrate between clouds;²⁷² others said it does not.²⁷³
- 7.48 A few customers said that providers could be more transparent about their services. For example:
- 7.49 A customer said some known issues may only become apparent after integration with a specific platform.²⁷⁴
- 7.50 Another customer said that it is not always clear to developers which features are common across all cloud platforms and which are proprietary steps could be taken by cloud providers to better inform customers in this respect, allowing for increased transparency and clarity.²⁷⁵

²⁶⁸ For example, BT's response to Ofcom's proposal to make a market investigation reference dated 17 May 2023.

²⁶⁹ [×].

²⁷⁰ Responses to CMA's information requests [>].

²⁷¹ Responses to CMA's information requests [>].

²⁷³ Responses to CMA's information requests [\times].

²⁷⁴ [\gg] response to CMA's information request [\gg].

²⁷⁵ [\times] response to CMA's information request [\times].

- 7.51 A customer said that it finds some cloud providers are more transparent than others, and lower levels of transparency can make integration between platforms more challenging.²⁷⁶
- 7.52 However, a customer said that available API documentation is usually good.²⁷⁷
- 7.53 Similarly, some cloud providers said that they provide extensive public documentation as well as training on their services (outlined previously in section 7), including that which instructs customers on integrating with, and switching to other platforms.²⁷⁸

Our emerging view

7.54 Based on the evidence we have seen to date, our emerging view is that a lack of transparency in supporting technical documentation can be a contributing factor that increases costs associated with integrating clouds or switching between clouds.

 $^{^{276}}$ [>] response to CMA's information request [>].

²⁷⁷ [>] response to CMA's information request [>].

 $^{^{278}}$ Responses to CMA's information requests [\times].

8. Mitigation of technical costs to multi-cloud and switching

- 8.1 In this section we discuss ways in which any technical multi-cloud and switching costs faced by customers could be mitigated and their impact lessened.
- 8.2 First, we set out evidence on the use of existing mitigations to technical costs. Second, we discuss the cloud providers' incentives to compete to develop mitigations in the future.

Current mitigations to technical costs

8.3 We start by outlining our understanding of the mitigations currently available to customers, then we present the evidence we have seen from cloud providers on the mitigations available on their public clouds and finally discuss the effectiveness of these mitigations from the customers' perspective.

Existing mitigations to technical challenges

- 8.4 Based on the evidence we have seen to date from customers, ISVs, and nonprofit organisations, we have identified four potential customer-led mitigations and two potential provider-led mitigations to technical challenges to multicloud and switching, which are explained below.
- 8.5 Use of cloud providers' services designed to facilitate multi-cloud and/or switching: All cloud providers told us that they offer services designed to facilitate multi-cloud. We understand that such services typically act as abstraction layers. All the major cloud providers said they offer technical (architectural design support) and non-technical (training and blogs) services to facilitate switching from other public clouds.
- 8.6 Use of adaptors: An adaptor is a small, focused piece of software that facilitates communication between two or more components that cannot directly interoperate with each other. Specifically, it translates and bridges communication by exposing the functionalities and/or data of one service to another. Adaptors are relevant to the technical costs arising from differentiation of interfaces for core and ancillary services, and asymmetry of integrations. Customers can procure adaptors from a third party or develop them internally.
- 8.7 Use of abstraction layers: Abstraction layers automate or simplify the operation of the cloud technologies that sit below them in the cloud stack (including services, tools, APIs, protocols and workflows), such that

customers do not need to configure them directly. Abstraction layers can be configured to simultaneously operate across different clouds and are therefore relevant to the technical costs arising from differentiation of features and integrations for core and ancillary services and tools. Customers can procure abstraction layers from a third party or develop them internally.²⁷⁹

- 8.8 Use of laaS and open-source software: As discussed in section 5, our evidence suggests that PaaS is more cloud-specific with more differentiated features and interfaces than laaS. Customers can therefore deploy laaS products with open-source alternatives of proprietary PaaS products or deploy either in isolation as part of their cloud architecture. Use of laaS and open-source software are relevant to the technical costs arising from differentiation of features and interfaces, and asymmetry of integrations in relation to core and ancillary services and tools. Customers can purchase laaS services from any cloud provider but typically have to procure and manage open-source software on their own.²⁸⁰
- 8.9 Use of cloud-agnostic services and tools from ISV: Some ISVs design their services and tools to have similar features and interfaces running on multiple public clouds. Such cloud-agnostic services and tools may mitigate technical challenges around differentiation of features and interfaces for core and ancillary services and tools.²⁸¹ Use of such services and tools that provide a consistent set of capabilities and interfaces across different clouds may also address transparency challenges but can increase the skills burden for customers, who must train or hire staff to manage the cloud-agnostic services and tools, in addition to the underlying cloud services.
- 8.10 Use of workarounds from cloud providers and ISVs: We have encountered technical workarounds designed by cloud providers and ISVs to support multicloud deployments by customers or make their services integrate with those of other cloud providers. However, we have not done a comprehensive exercise to develop a full list of these workarounds.

²⁷⁹ For example, we understand that some customers use 'platform engineering' in order to develop an abstraction layer over the cloud infrastructure services that are used by internal teams but procured at an organisational level (see for example 'What is Platform Engineering and why adopt it in your company? – CNCF Blog', accessed 14 May 2024).

²⁸⁰ Customers may also contract a supplier of professional services to help with the procurement and management of open-source software.

²⁸¹ ISVs cloud-agnostic services and open-source software may have similar effect on customers' ability to switch and multi-cloud. However, one key technical difference is how they are managed. Whilst ISVs' cloud-agnostic services are managed by the ISVs, the operations of open-source software is managed by the customer.

Use of cloud providers' services designed to facilitate multi-cloud and/or switching.

8.11 We outline below submissions from the major cloud providers on the services they provide to support multi-cloud and switching.

Evidence from AWS

- 8.12 AWS said it facilitates multi-cloud and switching in four ways: (i) building services using open-source technologies and standard protocols, including container technology; (ii) providing services designed to facilitate multi-cloud and/or switching; (iii) educating customers on building for 'reversibility' in their IT solutions; and (iv) allowing third parties to use AWS APIs and software development kits (SDKs) outside AWS.²⁸²
- 8.13 First, AWS said that its foundational compute and database services run on a range of open-source software and third party software which can be used on other cloud environments.²⁸³
- 8.14 Second, AWS said it has designed a wide array of technical solutions that facilitate multi-cloud and switching for customers.²⁸⁴ Additionally, AWS said it develops services to make integration across clouds easier and gave the example of a data source connector for Amazon Athena that customers can use to run SQL queries on data stored in virtually any format, wherever it resides.²⁸⁵
- 8.15 Third, AWS said that it regularly publishes blog posts dedicated to the topic of switching away from its public cloud. It also said it provides free courses and guidance on how to move workloads to or from AWS through the AWS Migration Acceleration Program.²⁸⁶
- 8.16 Finally, AWS said it makes many of its APIs and SDKs publicly available under open-source licences; uses open protocols, interfaces, APIs and data formats across services; and publishes extensive documentation, including, where relevant, differences between the AWS services and the underlying open-source. As an example, AWS said it offers an open-source solution called 'Mountpoint for Amazon S3' that allows customers to integrate Amazon S3 with any storage they use.²⁸⁷

²⁸² AWS' submissions to CMA [><].

²⁸³ AWS' response to CMA's information request [\gg].

²⁸⁴ AWS' submissions to CMA [\approx]. [\approx].

²⁸⁵ AWS' submissions to CMA [\times]. [\times].

²⁸⁷ AWS' submissions to CMA [>].

Evidence from Microsoft

- 8.17 Microsoft said that it facilitates multi-cloud and switching in several ways:²⁸⁸
- 8.18 First, Microsoft said it supports open-source software that facilitates switching and provided the examples of Linux and Kubernetes. It said it ensures its services are compatible and interoperable with other public cloud infrastructure services, by following industry standards and best practices, such as using open-source software, supporting open-source projects.²⁸⁹
- 8.19 Second, Microsoft said some of its services are designed to facilitate interoperability between clouds and provided the example of its service Azure Arc.²⁹⁰ Azure Arc allows customers to manage resources hosted outside Azure across on-premises, hybrid and multi-cloud environments from the Azure Portal as though they were hosted on Azure. Microsoft also said its cloud service Azure Fabric²⁹¹ can integrate data from disparate data sources across cloud environments to be used with Azure services, such as AI. ²⁹²
- 8.20 Third, Microsoft said it educates customers how to switch or integrate public clouds. It said it publishes information and training on its website (Microsoft Learn), including information to developers about the services available in Azure and how they can access their functionality.²⁹³ It also said it runs virtual and in-person training sessions.²⁹⁴
- 8.21 Finally, Microsoft said it helps with multi-cloud and switching by using common protocols and formats and providing APIs and SDKs for developers.²⁹⁵

Evidence from other cloud providers

8.22 We also reviewed evidence from Google, IBM and Oracle about their mitigations to technical challenges to customers' ability to multi-cloud and switching.

²⁸⁹ Microsoft's response to CMA's information request [×].

²⁹⁰ 'Azure Arc overview - Azure Arc | Microsoft Learn', accessed 23 May 2024; Microsoft's response to CMA's information request [><].

²⁹¹ 'What is Microsoft Fabric - Microsoft Fabric | Microsoft Learn', accessed 23 May 2024.

²⁹³ [>]. Microsoft's response to CMA's information request [>].

²⁹⁴ [\times]. Microsoft's response to CMA's information request [\times].

 $^{^{295}}$ Microsoft's response to CMA's information request [%].

- 8.23 Each of them said that they (i) provide API and SDK access to third parties;
 (ii) design product to be interoperable across clouds; and (iii) support or make available open-source software.²⁹⁶
- 8.24 Google said it also supports multi-cloud and switching by:
- 8.25 Offering public training and guidance to switch between cloud services or pursue a multi-cloud strategy with Google. It also offers numerous training modules on multi-cloud including its hybrid and multi-cloud architect learning path.²⁹⁷
- 8.26 Developing services specifically to support easy integration. It gave the example of Google Cloud Storage, which can integrate data from multiple sources and Google Cloud VMware Engine, which lets VMware customers adopt Google Cloud without making changes to applications or processes.²⁹⁸
- 8.27 Oracle also said one of the ways it supports multi-cloud is by collocating data centres with Microsoft Azure to reduce latency for customers who have cloud infrastructure with both providers.²⁹⁹
- 8.28 IBM said its cloud offering is based on a hybrid multi-cloud approach, meaning that IBM provides cloud-related services largely irrespective of the customers' choice of cloud service provider.³⁰⁰

Use of customer-led mitigations to technical challenges

- 8.29 This section sets out the evidence we have seen to date on how the first four mitigations are deployed by customers to support their ability to multi-cloud and switch.
- 8.30 To structure our analysis, we discuss each type of mitigation in separate subsections. However, there may be some overlap between abstraction layers, laaS and open-source, and cloud-agnostic tools since they are not entirely mutually exclusive categories.

Use of adaptors

8.31 A customer and a non-profit organisation said there are some hurdles to the use of adaptors.

²⁹⁶ Responses to CMA's information requests [>].

²⁹⁸ Google's response to CMA's information request [\approx].

²⁹⁹ Oracle's response to CMA's information request [\times].

- 8.32 The customer said that 'application integration' services that are designed to smooth API interoperability 'seem interesting' but are still too complex. This customer deployed an internal network tool to act as a bridge across its cloud providers but said that 'even that comes at a cost'.³⁰¹
- 8.33 The non-profit organisation said that proprietary APIs reduce developers' willingness to create adaptors that work with these APIs as these may be covered by method-patents.³⁰²
- 8.34 We note that customers bear the additional cost of developing or purchasing an adaptor. To develop their own adaptor, customers would incur costs, such as development and testing costs. Alternatively, customers would incur a cost when purchasing an adaptor or a service that supports an adapter from a cloud provider or another party. For example, a customer would need to have an Amazon S3 subscription to use the built-in S3 adapter that can connect Amazon Kinesis Video Streams to a non- AWS service,³⁰³ adding an additional service purchase requirement for the customer.

Use of abstraction layers

- 8.35 From the evidence we have seen to date, customers tend to deploy Infrastructure as Code (IaC) as their preferred abstraction layer for multi-cloud operations. IaC is the use of high-level descriptive coding language to automate and standardise the provisioning and deployment of IT infrastructure such as networks, virtual machines, load balancers, and connection topologies required by any application.³⁰⁴
- 8.36 Terraform (by Hashicorp) is the most cited abstraction layer used by customers. While initially Terraform's source code licence was open source, as of 2023 it has moved to a business source license.³⁰⁵
- 8.37 Some customers, a non-profit organisation and the Jigsaw report noted that abstraction layers, like IaC platforms, enable multi-cloud deployments through improving the interaction between different cloud provider APIs and standardising the infrastructure deployment across clouds.³⁰⁶ For example, a customer said it uses Terraform as a 'common language' to standardise the operating model across multiple clouds, while another customer said it uses

³⁰¹ [\gg] response to CMA's information request [\gg].

³⁰² Note of meeting with [>].

³⁰³ 'AWS Kinesis Video Streams, Integration manual', accessed on 12 December 2023.

³⁰⁴ 'What Is Infrastructure as Code (IaC)? | IBM'; What is infrastructure as code (IaC)? - Azure DevOps | Microsoft Learn, accessed 1 May 2024.

 $^{^{305}}$ [\gg] response to CMA's information request [\gg].

³⁰⁶ Responses to CMA's information requests [%]; Notes of meetings with [%].
open-source tools like Ansible to abstract cloud provider APIs.³⁰⁷ The nonprofit organisation said that tools like Terraform have been developed to overcome the absence of standardised cloud provider APIs.³⁰⁸

- 8.38 Similarly, a few customers, a few ISVs and a supplier of professional services said that Terraform and similar products improve their ability to manage their multi-cloud architecture and improve overall efficiency.³⁰⁹
- 8.39 One of these customers said that Terraform is a good tool for abstracting the differences between cloud providers, and that the ability to use Terraform on different clouds is a strength, as it is an extensible format and providers generally add support for new services, which means that it can be used to deploy any service.³¹⁰
- 8.40 Similarly, a supplier of professional services said innovations in Terraform, and similar services, simplify the complexity of provisioning and maintenance of management services which would allow ISVs to consolidate their own efforts.³¹¹
- 8.41 However, a few customers and an ISV said there are multiple costs to be considered when deploying IaC tools.³¹²
- 8.42 A customer said deploying Terraform would be another skill that developers would need to learn, creating further costs for a customer to train or hire new staff.³¹³
- 8.43 Similarly, the ISV said it is unlikely to internally develop a comparable abstraction itself because it would require shifting capital and labour resources away from other mission-critical projects and potentially increase risks.³¹⁴
- 8.44 Additionally, a customer, a market research and advisory organisation, and a cloud provider said deploying third party abstraction layers can create vendor-specific lock-in.³¹⁵

- ³¹² Notes of meetings with [\times].
- ³¹³ Note of meeting with [%].
- ³¹⁴ Note of meeting with [%].

³⁰⁷ [\gg] response to CMA's information request [\gg]; Note of meeting with [\gg].

³⁰⁸ Note of meeting with [>].

³⁰⁹ Notes of meetings with [\times]; [\times] response to CMA's information request [\times].

³¹⁰ Note of meeting with [>].

³¹¹ Note of meeting with [\gg].

- 8.45 The market research and advisory organisation said IaC tools like Terraform or Pulumi must specify configurations that are unique to individual cloud providers and, therefore, do not result in portability.³¹⁶
- 8.46 Separately, the cloud provider said that Hashicorp's announcement in 2023 to change its source code licence from Mozilla Public License v2.0 (ie open-source license) to the Business Source License has the potential to impact all third party use of Hashicorp products, particularly Terraform.³¹⁷
- 8.47 The Jigsaw report also found that even cloud-agnostic IaC tools can require provider-specific configurations, which means that the main technical barrier for customers to multi-cloud or switch persists³¹⁸ and building an abstraction layer while still using provider-specific PaaS required a substantial amount of effort by them.³¹⁹

Use of IaaS and open-source software

- 8.48 Some ISVs and a customer said they use open-source software to support multi-cloud and switching. They said that the use of open-source software was motivated by the increased scope of portability, relative to relying on proprietary PaaS offerings.³²⁰
- 8.49 Similarly, a few customers and an ISV said that using generic IaaS services increased their ability to switch between different clouds.³²¹
- 8.50 The ISV said that using a minimum number of proprietary functionalities allowed it to design their flagship product in a manner that could be ported to a private cloud, which it estimated to save it USD 20 million annually. However, it said that despite using this mitigation, the process of migration was onerous.³²²
- 8.51 A customer said the ability to port workloads across providers was increased by using these tools since they needed minimal changes during switching. It also said services, like PaaS, are not standardised and need adaptations to be ported to another provider.³²³

³¹⁶ [\gg] response to CMA's information request [\gg].

³¹⁷ [\gg] response to CMA's information request [\gg].

³¹⁸ Cloud Services Market Investigation Qualitative Customer Research conducted by Jigsaw (2024), paragraph 4.4.17.

³¹⁹ Cloud Services Market Investigation Qualitative Customer Research conducted by Jigsaw (2024), paragraph 4.1.13.

³²¹ [\gg] submission to CMA [\gg]; Responses to CMA's information requests [\gg].

 $^{^{322}}$ [>] submission to CMA [>].

³²³ [>] response to CMA's information request [>].

- 8.52 However, some customers highlighted the trade-offs customers face when deciding whether to use laaS and open-source services instead of proprietary PaaS alternatives.³²⁴
- 8.53 Some of these customers said that using PaaS provided the most benefits of being in the cloud. In their view, using IaaS or self-managed services would prevent them from accessing the innovations and potentially increase the risk of financial loss and loss of critical features.³²⁵ For example, a customer said that using open-source platforms could also reduce the benefits and value of using the cloud, as customers would not leverage the specialised and differentiated features and capabilities that providers offer.³²⁶
- 8.54 A customer said adopting open-source technologies is challenging in an environment where cloud providers promote and advance their proprietary capabilities.³²⁷
- 8.55 Another customer said open-source alternatives are harder to scale than bespoke database solutions such as DynamoDB because they are built for running on a local machine, and therefore utilising some open-source alternative would increase cost.³²⁸
- 8.56 Another customer said that it generally prefers using managed versions of open-source software where it is a part of one if its customer-facing solutions, as opposed to the community versions despite the increased risk of vendor lock-in due to the operational risk, skill and the time required to do so.³²⁹
- 8.57 A supplier of professional services said that while working with open-source software, customers should understand that they are trading service portability for continuous management and support, and that they must rely on a community for understanding and using the tool.³³⁰

Using cloud-agnostic services and tools from ISVs

8.58 We have heard from market participants that there are a wide variety of cloudagnostic services and tools from ISVs that can mitigate against cloud lock-in.

 $^{^{324}}$ Responses to CMA's information requests [%]; Notes of meetings with [%].

 $^{^{325}}$ Responses to CMA's information requests [\Join].

³²⁶ [>] response to CMA's information request [>].

 $^{^{327}}$ [\gg] response to CMA's information request [\gg].

³²⁸ Note of meeting with [\gg].

³²⁹ Note of meeting with [>].

³³⁰ Note of meeting with [>].

- 8.59 A customer said there is a cloud-agnostic ISV tool for every type of tool it needs and that it takes this approach with tools that need to be used often.³³¹
- 8.60 An ISV said it uses a cloud-agnostic billing tool, Flexera, to manage its billing processes across the three major cloud providers.³³²
- 8.61 However, a customer, a market research and advisory firm, and a provider of professional services said that deploying cloud-agnostic tools increases the management and commercial overhead associated with such tools, forcing customers to choose between service portability and functionality.³³³
- 8.62 For example, the market research and advisory firm said a cloud-agnostic tool will rarely have the same breadth and depth of functionality across all clouds.³³⁴
- 8.63 The provider of professional services said that some ISVs work better in certain clouds adding an additional layer of lock-in.³³⁵
- 8.64 Additionally, a non-profit organisation and a provider of professional services said that using cloud-agnostic ISVs can still lead to lock-in.³³⁶ The non-profit organisation said customers developing cloud-agnostic applications have to use the lowest common denominator of services and have the knowledge and capabilities within their company to do so. However, lock-in can happen because the skills are lost through a reliance on cloud providers' services to provide these capabilities.³³⁷
- 8.65 Finally, a few customers said there are significant costs associated with internally developing such cloud-agnostic tools.³³⁸ As an example, a customer said that for a hypothetical application workload that costs £1m to develop, it might cost £200,000 to ensure that the workload could be easily switched between public clouds.³³⁹ It further stated that ISVs that offer ancillary tools/services, such as CloudHealth, must constantly play 'catch up' with the changes providers make to their underlying cloud services and the associated cost models.³⁴⁰

³³⁹ Note of meeting with [\gg]. ³⁴⁰Note of meeting with [\gg].

³³¹ Note of meeting with [>].

³³² Note of meeting with [>].

³³³ Responses to CMA's information requests [\times]; Note of meeting with [\times].

 $^{^{334}}$ [>] response to CMA's information request [>].

³³⁵ Note of meeting with [\gg].

 $^{^{336}}$ Notes of meetings with [>].

³³⁷ Note of meeting with [>].

³³⁸ Note of meeting with $[\times]$; $[\times]$ response to CMA's information request $[\times]$.

Containers and Kubernetes

- 8.66 Containers are an example of a cloud-agnostic architecture that has become popular with customers. These lightweight packages of application code house the dependencies required to run software services in the cloud, such as specific versions of the programming language runtimes and libraries. Since containers package all the dependencies needed to run an application within an object, customers can easily deploy applications across multiple clouds.
- 8.67 To streamline orchestration of these containerised applications, customers have deployed Kubernetes, which is a portable, extensible, open-source platform for managing containerised workloads and services, that facilitates declarative configuration and automation.³⁴¹ By providing automated container orchestration, Kubernetes improves reliability and reduces the time and resources attributed to daily operations.³⁴²
- 8.68 Some customers said that they use containers to improve the portability of their workloads.³⁴³
- 8.69 As an example, a customer said that using containers helps it to manage applications across its multi-cloud environment.³⁴⁴
- 8.70 Another customer said that it uses Kubernetes to develop applications in a faster and more streamlined manner while being able to retain their transportability.³⁴⁵
- 8.71 Another customer said Kubernetes and other technical solutions provide open APIs which it has used to provide workload mobility across technology platforms.³⁴⁶
- 8.72 However, some customers, a supplier of professional services and a market research firm said containers are not completely effective at overcoming barriers towards multi-cloud and switching since the underlying infrastructure and supporting ancillary services are built on proprietary provider technology, making a simple lift-and-shift difficult.³⁴⁷
- 8.73 For example, the supplier of professional services said that containers don't make workloads portable because of the dependencies to the larger cloud

³⁴¹ Overview | Kubernetes, Accessed on 2 May 2024.

³⁴² What Is Kubernetes? | Google Cloud, Accessed on 2 May 2024.

³⁴³ Responses to CMA's information requests [\succ].

³⁴⁴ [\succ] response to CMA's information request [\succ].

³⁴⁵ [\approx] response to CMA's information request [\approx].

³⁴⁶ [\times] response to CMA's information request [\times].

³⁴⁷ Notes of meetings with [\approx]; [\approx] response to CMA's information request [\approx].

system. It said that containers are dependent on security, monitoring, storage in the wider cloud, and have many integration points with each of these services. ³⁴⁸

8.74 A customer said that the use of open-source abstraction technologies like Kubernetes increased the management costs and required significant upfront investment, and can lead to 'greater system complexity, which can have unintended negative impacts, such as reduced platform stability and increased complexity of change'.³⁴⁹

Use of provider-led mitigations to technical challenges

Use of cloud provider and ISV workarounds

- 8.75 We have evidence from ISVs and cloud providers that have designed workarounds to allow customers to integrate with other cloud providers.
- 8.76 A cloud provider said it has developed one-way technical workarounds that only partially address customer challenges presented by Microsoft's refusal to support interoperability between Microsoft Active Directory, and third party Identity as a Service tools.³⁵⁰
- 8.77 An ISV said it has developed abstractions for its service that map to fundamental services available in each cloud provider.³⁵¹
- 8.78 Another cloud provider said that if the application needs to use a data warehouse (a service such as Google BigQuery), data (including data types, schemas and formats) will need to be converted to those used by the specific data warehouse (BigQuery here) which differ from those of other warehouse services.³⁵²
- 8.79 The above is a preliminary list of workarounds that we have observed. We welcome views and evidence from parties on other workarounds that facilitate multi-cloud and switching.

Our emerging views

8.80 Based on the evidence we have seen to date on customer-led mitigations we consider that there are various tools and approaches that customers can use to mitigate lock-in, but they may incur additional costs for customers and may

³⁴⁸ Note of meeting with [>].

³⁴⁹ [\approx] response to CMA's information request [\approx].

 $^{^{350}}$ [>] response to CMA's information request [>].

³⁵¹ Note of meeting with [>].

lead to increased reliance on ISVs. Mitigations are more likely to be deployed by larger customers, while small and medium-sized customers may have to choose between interoperability/portability and cost minimisation.

- 8.81 For provider-led mitigations, evidence we have seen to date leads us to consider that:
- 8.82 Cloud provider services at the infrastructure level seem to better support multi-cloud and switching, but as customers buy into PaaS products their ability to port is significantly lowered. The provision of managed open-source software by cloud providers seems to reduce management costs for customers but may lock them into the cloud provider's cloud ecosystem through integrations with other PaaS and ancillary services.
- 8.83 Despite the major cloud providers stating their products are designed for multi-cloud and switching, the need for ISVs and other cloud providers to create technical workarounds to facilitate integration with several services indicate the presence of technical costs for customers, smaller cloud providers and ISVs.
- 8.84 We have limited evidence of customers utilising or benefitting from providerled mitigations but have observed their presence.
- 8.85 Overall, these mitigations might not effectively support efficient multi-cloud and switching for customers. We welcome comments on the uptake and effectiveness of customer and provider-led mitigations.

Cloud providers' incentives to compete on mitigating technical challenges

- 8.86 In addition to mitigation strategies that are currently available to customers, we have also considered cloud providers' incentives to develop mitigations in the future, ie to take actions or technical design decisions for products and services to lower the technical cost of interoperating with other public clouds and switching between public clouds. If current mitigations are not sufficient but cloud providers have the right incentives to develop new mitigations in the future, the market alone may be able to address the technical challenges to multi-cloud and switching that customers may be facing.
- 8.87 We first set out the views of the large cloud providers, AWS and Microsoft, on their incentives to interoperate and thus facilitate multi-cloud and switching. We then set out our initial assessment of such incentives for all cloud providers and our emerging views.

Evidence from cloud providers

- 8.88 The large cloud providers, AWS and Microsoft, told us that they are incentivised to make their public clouds interoperable.
- 8.89 AWS said that it is incentivised to support interoperability by customer demands and preferences. It said that customers are often highly sophisticated and will ensure that the IT environment they are purchasing will meet their needs, including on the ability to use multiple cloud providers. AWS said that customers demand the flexibility to incorporate third party technology and services into their IT solutions because they know that no single IT provider can ever be a 'one-stop-shop', offering native IT solutions for every use-case. If customers are not confident that they will be able to do so when the next innovation is released, or when they need a niche solution, they will not choose AWS.³⁵³
- 8.90 Microsoft said that its position, as a challenger to AWS in the cloud services market, means that it has always been incentivised to make it as easy as possible for customers to switch to Microsoft (in particular, from AWS) or to multi-cloud as customers focus on diversifying beyond AWS. It said it is not possible for Azure to implement a lopsided portable system to be both seamless to switch into and hard to move out of. Microsoft said it also has an incentive to increase the extent of interoperable services in order to maximise customers' usage of Azure infrastructure, but must balance that interest against the need to continue to deliver more innovative and performant cloud services to its customers. It said that customers are sophisticated buyers with specialised knowledge, procurement teams and resources, making informed decisions on the technical and commercial structure of their cloud deployments.³⁵⁴
- 8.91 In addition, AWS and Microsoft said that they are incentivised to facilitate interoperability because of pressure from open-source communities and synergies with open-source software. For example:
- 8.92 AWS said that it updated its EC2 service to support the open virtualisation format (OVF) in 2013, which 'allowed users to package EC2 instances in a format widely recognised in the virtualisation community, fostering smoother transitions across different IT providers that support OVF'. AWS also said that interoperability through open standards and open-source software can reduce

³⁵³ AWS' response to the Issues Statement, 17 October 2023, paragraph 18; AWS' submission to CMA [\approx]; AWS' response to CMA's information request [\approx].

³⁵⁴ Microsoft's response to the Issues Statement, 17 October 2023, paragraphs 26-32.

costs for both providers and customers, since open-source software is often developed by a community where the development costs are shared.³⁵⁵

- 8.93 Microsoft said that it was incentivised to make Azure Arc interoperable with existing standards in keeping with the open-source community's expectation of an open source solution to multi-cloud management, and also to avoid customer perception of Azure Arc as a mechanism to lock them in the Azure ecosystem.³⁵⁶
- 8.94 Cloud providers have submitted examples of mitigations they have implemented.³⁵⁷ However, many of these examples relate to cloud providers' incentives to interoperate with customers' on-premises IT and within their respective public cloud ecosystem, as opposed to their incentive to interoperate with other public cloud ecosystems.
- 8.95 Evidence we have seen from cloud providers supports this:
- 8.96 A cloud provider said in an internal document that it 'believes container portability could lead to more customers operating in multiple clouds', but it 'will double down on containers in spite of the risks because it will quicken the migration of traditional workloads' towards it.³⁵⁸
- 8.97 Another cloud provider said in an internal document that one of its infrastructure priorities for the 2023 financial year was to win new hybrid customers: enable customers to govern, manage and secure their entire digital estate across its platform, on-premises and edge, as well as build new cloud native apps with its services.³⁵⁹

Our initial assessment

8.98 As an initial observation, it does not necessarily follow that just because customers would value interoperability between public clouds, cloud providers are incentivised to take actions or technical design decisions for products and services to reduce technical costs for multi-cloud and switching. While reducing such costs may allow cloud providers to win more incremental customers and/or workloads from their rivals, it may also increase the risk that these cloud providers lose customers and/or workloads to their rivals, or that

³⁵⁵ AWS' submission to CMA [\succ].

³⁵⁶ Note of meeting with Microsoft [>].

³⁵⁷ This includes offering open-source software in some cloud infrastructure services (eg Linux operating system in Amazon EC2), support for cloud-agnostic services by ISVs (eg MongoDB) and support for containers (eg Kubernetes). See discussion earlier in this section on whether these services and software may mitigate the technical multi-cloud and switching cost that customers may be experiencing.

³⁵⁸ [\times] response to Ofcom's information request [\times].

these cloud providers would have to offer more competitive prices, quality or levels of innovation in order to retain them.

- 8.99 The extent to which cloud providers are incentivised to reduce technical costs to multi-cloud and switching may be associated with their shares of supply. The larger the existing share of supply held by a cloud provider, the larger is the pool of revenues and profits from which they may lose incremental customers and/or workloads, and the smaller is the pool of revenues and profits from which they may lose incremental customers and/or workloads.
- 8.100 Another factor which may affect the cloud providers' incentives to reduce technical costs to multi-cloud and switching may be the level of their market power. For example, cloud providers with the large shares of supply, may have more to lose from customers using multi-cloud architectures and switching, as this could over time erode their ability to sustain higher levels of profitability. We consider the market power of cloud providers in our Competitive Landscape working paper.
- 8.101 We also note that there is a dynamic element to cloud providers' incentives to reduce technical costs to multi-cloud and switching. As noted, in our Competitive Landscape working paper, cloud providers with large shares of supply may have a stronger incentive now than in the future to compete for customers and workloads that are new to the public cloud. This is because winning customers in the present may allow them to establish a stronger position in the future. Whilst potential customers considering migrating from on-prem to cloud may value the absence of lock-in and give cloud providers a possible incentive to facilitate switching and multi-cloud, these incentives may be weaker or changed in a future where a lot of the migration to cloud has occurred.
- 8.102 We also note that customers may find it relatively easy to migrate a workload to a public cloud, but still difficult to integrate it with other public clouds or switch away. This is because a customer that migrates a workload from its legacy IT systems to the cloud, would typically 'lift and shift' that workload to laaS services, and then refactor it to improve its suitability to the cloud, including replacing parts of the workload with PaaS services. As discussed in section 5 of this paper, PaaS services, particularly those that are proprietary, may create more lock-in than using laaS services with equivalent self-managed software.³⁶⁰

³⁶⁰ In the case of cloud-native workloads, customers typically develop these on a public cloud in the first place, so this does not affect cloud providers' incentives.

- 8.103 Overall, cloud providers face a complex mix of incentives when deciding whether or not to support multi-cloud and switching. Because of this, the simple observation that customers value interoperability may be insufficient, of itself, to give a clear indication of the overall strength of providers' incentives to provide high levels of interoperability. There is likely to be significant complexity and uncertainty around attempting to decompose these incentives into the relevant gains and losses.
- 8.104 We welcome views and evidence on the above and on what other factors may influence cloud providers' incentives to lower technical costs to multi-cloud and switching. We are particularly interested in whether, and the extent to which:
 - (a) cloud providers can and do design public cloud infrastructure services in a way which makes it easy to switch to but hard to switch away from at a technical level;
 - (b) other cloud providers, ISVs and customers can unilaterally mitigate technical costs to multi-cloud and switching, without the active co-operation of the incumbent cloud providers; and
 - (c) open-source communities are able to incentivise cloud providers to facilitate multi-cloud and switching, for example because these communities develop more open competing products, or because customers and/or cloud providers' employees share their values and are able to influence cloud providers.

9. Potential remedies

Introduction

- 9.1 In the event that we find that technical barriers are a feature that gives rise to an AEC, we are required to decide whether, and if so what, remedial action should be taken to address that AEC.³⁶¹ In this section we outline our emerging views on potential remedies relating to technical barriers.
- 9.2 We described the CMA's approach to remedies in our issues statement.³⁶² We are at an early stage of considering potential remedies and as our understanding of the market(s) and the potential issues develops, we expect our consideration of potential remedies to evolve. As set out in the CMA's guidance,³⁶³ we will consider and discuss potential remedies alongside working on understanding what features of the market may give rise to adverse effects. Consistent with this, we set out in this section our early views on potential remedies to any potential AEC(s) relating to technical barriers and invite submissions from parties on these to help inform our emerging views.
- 9.3 We also note that we are considering the potential for cross-cutting remedies or a package of remedies which would combine to remedy, mitigate or prevent any AECs or their detrimental effects on customers.³⁶⁴

Overview of potential remedies to technical barriers

- 9.4 The potential remedies that we discuss in this working paper would aim to do one or more of the following:
 - (a) increase the degree of standardisation of cloud services and/or interfaces, to increase interoperability and portability of cloud services, through voluntary standards, mandatory standards or principle-based requirements.
 - (b) improve the interoperability of cloud services, through the use of abstraction layers;
 - (c) increase interconnectivity and reduce latency;
 - (d) increase transparency around the interoperability of cloud services; and

³⁶¹ Section 134(4) of the Enterprise Act 2002.

³⁶² Issues statement (publishing.service.gov.uk)

³⁶³ CMA3 Revised), Market Studies and Market Investigations: Supplemental guidance on the CMA's approach (publishing.service.gov.uk), paragraph 3.50. ³⁶⁴ Issues statement (publishing.service.gov.uk), paragraphs 57 and 58.

(e) improve the portability of skills between cloud providers.

General design considerations for potential remedies to technical barriers

- 9.5 We have identified four general considerations for the design of potential remedies to technical barriers:
 - (a) the cloud services and/or interfaces that would be within scope of a potential remedy;
 - (b) the cloud providers that would be within scope of a potential remedy;
 - (c) the duration of a potential remedy; and
 - (d) any interactions with remedies outside of the UK.

Cloud services and/or interfaces that would be in scope

9.6 When considering potential remedies, particularly for those seeking to increase standardisation and/or to improve interoperability, we consider the cloud infrastructure services that would be in scope. Some potential remedies could relate to all cloud infrastructure services, others to all IaaS, all PaaS, all core services or all ancillary services and tools, whereas others may be specific to an individual cloud infrastructure service.

Cloud providers that would be in scope

- 9.7 The cloud provider(s) that would be in scope for any remedies could also vary depending on the specific remedy under consideration. For example, a remedy, or part of a remedy, that only applies to laaS services could be limited to providers of laaS or to a subset of providers of laaS.
- 9.8 We also note that there are certain general approaches that we could adopt. For example, potential remedies could be limited to:
 - (a) the largest providers or
 - (b) all cloud providers who exceed a pre-determined threshold (for example a pre-determined threshold based on UK or global revenue).
- 9.9 When considering whether to limit a potential remedy to the largest cloud providers or a subset of cloud providers (but not all), we will assess the extent to which the associated costs might have a disproportionate effect on smaller cloud providers.

Duration

- 9.10 We will consider the duration of any potential remedy. The duration could be:
 - (a) unlimited;
 - (b) a fixed time period, at the end of which we would review whether the remedy should be retained or lapse; or
 - (c) when certain conditions are met and the remedy is no longer required.

Interactions with regulations outside the UK

EU Data Act

- 9.11 The EU Data Act governs the use and exchange of data within the EU and contains provisions on interoperability and technical barriers.
- 9.12 The provisions on interoperability and technical barriers come into force on 12 September 2025. We are not currently aware of any actions taken by cloud providers in response to the provisions on interoperability and technical barriers.
- 9.13 We will monitor the cloud providers' responses to the obligations placed on them under the EU Data Act, insofar as the obligations under the EU Data Act are also relevant to our consideration of potential remedies.
- 9.14 We note that it is not mandatory for cloud providers to extend any actions that they take in response to the EU Data Act to the UK. Therefore, as part of our assessment of potential remedies, we may consider whether actions taken in response to the EU Data Act should also apply to the UK.

Remedies requiring cloud providers to increase standardisation

9.15 In this section, we consider potential remedies to increase standardisation of cloud services and interfaces. Where relevant, we have considered core services, ancillary services and tools and interfaces separately.

Potential remedies that require common standards for cloud providers

9.16 We understand that common technical standards already exist to facilitate interoperability for some cloud services and the associated interfaces. We are also aware that the levels of adoption of these common technical standards varies between different cloud services and interfaces and between different cloud providers.

- 9.17 This potential remedy requires cloud providers to follow common standards for some or all cloud services and interfaces. The potential remedy could require cloud providers to contribute to the development of new standards or to adopt existing standards.
- 9.18 We recognise that standards may be more appropriate for some cloud services and interfaces than others. We also note that standards could vary from one type of cloud service or interface to the next but would broadly attempt to set minimum technical requirements to improve interoperability and portability.
- 9.19 Common standards could be:
 - (a) voluntary to allow cloud providers to coalesce around common technical requirements, but with a backstop of mandatory standards if no agreement is reached; or
 - (b) mandatory meaning that cloud providers would be mandated to adopt the standards.

Stakeholder views

- 9.20 IBM suggested open industry-supported standards with appropriate governance.³⁶⁵
- 9.21 A cloud provider said that the lack of open and widely used standards limits the interoperability and portability of applications. It also said that it can take time to implement common standards.³⁶⁶
- 9.22 We have seen academic research that suggests that:
 - (a) There is currently no incentive for cloud providers to adopt voluntary standards since it would decrease their competitive advantage and make it easier for customers to switch.³⁶⁷
 - (b) Calls for standardising cloud computing have had little impact on an increasing trend of differentiation in cloud services.³⁶⁸

³⁶⁵ IBM response to the issues statement, 17 October 2023.

³⁶⁶ [>] response to CMA's information request [>].

³⁶⁷ Yang, Z et al. (2023), 'SkyPilot: An Intercloud Broker for Sky Computing', Proceedings of the 20th USENIX Symposium on Networked Systems Design and Implementation, pages 437-455. ³⁶⁸ Stoice, Land Shenker, S (2021), 'Erom Cloud Computing to Sky Computing', Proceedings of the Workshop

³⁶⁸ Stoica, I and Shenker, S (2021), 'From Cloud Computing to Sky Computing', Proceedings of the Workshop on Hot Topics in Operating Systems HotOS '21), pages 26-32.

9.23 Another cloud provider said that if cloud providers are expected to facilitate customers achieving equivalence of outputs³⁶⁹ when they move cloud providers, it would delay or increase the cost of innovation, as cloud providers would need to take into account how the new development may impact on a customer's ability to achieve equivalence of outcomes.³⁷⁰

Design considerations for potential remedies involving setting common standards

Scope

- 9.24 Common standards could apply to the design and functionality of cloud services, or to the interfaces (eg APIs) that customers, ISVs, and other parties use to access and integrate cloud services.
- 9.25 The evidence that we have seen to date indicates that the existence and adoption of common standards varies between different IaaS, PaaS, ancillary cloud services and tools and the associated interfaces.
- 9.26 In Table 9.1, we comment on the adoption of standards for various cloud services and interfaces.

Table 9.1: Commentary on the extent to which common standards exist for different types of cloud service and interface

General category of cloud service or interface	Extent to which common standards have been adopted
laaS	The evidence that we have seen to date indicates that solutions compatible with Amazon's Simple Storage Service S3) are used extensively throughout the industry. ³⁷¹ However, some stakeholders noted that Azure Blob Storage uses different APIs which reduces interoperability with S3. ³⁷²
	More broadly, the evidence that we have seen to date indicates that cloud providers offer generally similar features in their core laaS services, but some customers found significant differences in the way features of those services function, ³⁷³ which could be indicative of limited use of common standards.
PaaS	There appears to be more limited use of common standards for more abstracted PaaS products and services.
Interfaces (APIs)	The evidence that we have seen to date indicates that different cloud providers use different APIs and this leads to reduced substitutability and/or interoperability. ³⁷⁴
Within ancillary services and tools specifically:	
Identity and access management	There is broad adoption of identity standards (eg SAML) but we have seen less evidence of industry coalescing around common standards for access management. ³⁷⁵

³⁶⁹ We define equivalance of outputs at paragraph 9.33 below.

 $^{^{370}}$ [>] submission to CMA [>].

³⁷¹ Paragraph 5.59

³⁷² Paragraph 5.54

³⁷³ Paragraph 5.31

³⁷⁴ Paragraphs 5.37 to 5.49

³⁷⁵ Paragraphs 6.30 and 6.45

General category of cloud service or interface	Extent to which common standards have been adopted
Observability	Industry may be moving towards adopting some common standards (eg Open Telemetry). ³⁷⁶
Provisioning and orchestration	Some common open-source technologies exist (ie Terraform and Kubernetes) and the evidence we have seen to date suggests that their take-up is increasing. ³⁷⁷
Billing	The evidence that we have seen to date indicates that there is limited adoption of common standards, which could contribute to potential difficulty in comparing billing data between cloud providers. ³⁷⁸

Source: CMA analysis

- 9.27 In general, the more abstracted a service is from the physical infrastructure, the more potential there is for greater differentiation between services of the same type. The consequence of this is that IaaS services tend to be more homogenous than PaaS services. This also means that within PaaS, lower abstraction PaaS services (eg container orchestration services) tend to have less differentiation between services than higher abstraction PaaS services (eg FaaS services).
- 9.28 Standards (and standardisation more generally) may be more appropriate for services that have a lower level of abstraction from the underlying hardware, such as storage and container orchestration services. Services with lower level of abstraction tend to be fundamental for the operation of the public cloud with many other services relying on them, which suggests that there may be greater benefits to competition and customers to reducing differentiation between them. This is consistent with the analysis in Table 9.1 which indicates that Amazon S3 and Kubernetes are commonly used by the industry as templates for storage and container orchestration services .
- 9.29 Standardisation may also be more appropriate for some ancillary services and tools, such as billing, because in general there appears to be lower levels of innovation with these services and tools, when compared to other cloud services, such as PaaS services.
- 9.30 The Jigsaw report found that challenges migrating databases and storage services are among the most commonly raised issues by customers. It may be appropriate to limit standardisation of interfaces to APIs used by databases and storage services or to all IaaS services, rather than to all cloud services.³⁷⁹

³⁷⁹ Cloud Services Market Investigation Qualitative Customer Research conducted by Jigsaw (2024) page 61.

³⁷⁶ Paragraphs 6.70 to 6.73

³⁷⁷ Paragraph 6.84

³⁷⁸ Paragraphs 6.62 to 6.68

Other design considerations

- 9.31 The standards could apply to all cloud providers or to a subset of cloud providers.
- 9.32 The standards could be technically simpler, such as standardising naming conventions for billing services and tools, or more complex, such as setting detailed technical requirements for access management.
- 9.33 Standards could require:
 - (a) Mandating participation in existing industry schemes or adopting common practices, for example, requiring cloud providers to publish some or all of their APIs.
 - (b) Equivalence of input this is what Ofcom refers to as a 'complementary equivalence requirement'³⁸⁰ and would require cloud providers to provide equivalent access to their cloud services, for example we could require cloud providers to standardise open APIs to support third party inputs.
 - (c) Equivalence of output a cloud service may look and operate differently, but the output is comparable between cloud providers. This is consistent with the requirement for 'functional equivalence' under the EU Data Act.³⁸¹
 - (d) Standardisation of functionality this would require cloud providers to ensure that the services are functionally the same (ie the input, the way the service operates, and the output is the same). While there are risks with this approach, there may be some circumstances where it merits further consideration, for example billing services.
- 9.34 We note that there may be circumstances whereby setting requirements around the functionality may be insufficient and we might also need to specify some or all of the terms around the access to these services. For example, this might apply in circumstances where IaaS (and/or PaaS) provides a key input into other services, and cloud suppliers have the ability and incentive to restrict access to these.
- 9.35 Setting and maintaining relevant standards would be vital for the effectiveness of a standardisation remedy, and our current view is that this would need to be performed by an independent body rather than through self-regulation.

³⁸⁰ Cloud services market study final report (ofcom.org.uk), paragraph 10.36.

³⁸¹ Providers of Infrastructure as a Service must take measures to facilitate that, where a customer switches to a service of the same type, the customer gets materially comparable outcomes in response to the same input for features that both services share 'functional equivalence'). Data Act explained | Shaping Europe's digital future (europa.eu); and Regulation - EU - 2023/2854 - EN - EUR-Lex (europa.eu), paragraph 86.

- 9.36 The independent body would consult with cloud providers and other stakeholders before setting the standards.
- 9.37 Different independent bodies could be appointed to set and monitor standards for different types of cloud service.

Potential impact

- 9.38 When considering the applicability of standards as potential remedies, we consider several factors, which include:
- 9.39 Current levels of adoption ie the extent to which the industry:
 - (a) has already adopted standards;
 - (b) is moving towards adopting standards; or
 - (c) is yet to coalesce around standards.
- 9.40 The extent to which standards have been adopted in relation to the provision of cloud services and interfaces appears to vary. There also appears to be different levels of adoption between the various ancillary services and tools.
- 9.41 Innovation the extent to which requiring cloud providers to adopt common standards could improve or reduce innovation. This may vary between cloud services and interfaces.
- 9.42 Access to and independence of standards setting bodies the extent to which a common standards body exists or could be created and is both capable and willing to oversee the design and implementation of the standards, as well as to ongoing maintenance.

Potential for unintended consequences

- 9.43 Where standards already exist or are under consideration, there is a risk of introducing competing standards. Competing standards may be counter-productive, adding complexity and ambiguity to the market.
- 9.44 There is a risk that by setting standards, we could impair innovation:
 - (a) by restricting the cloud services that could be developed due to requirements to ensure standardisation; or
 - (b) in the development of standards themselves.
- 9.45 There is also a risk that the standards-setting body:

- (a) may not be sufficiently informed and that the standards set may not represent an optimal solution. This risk applies more to mandatory standards and less to voluntary standards, as the market is less likely to adopt sub-optimal voluntary standards; and
- (b) is not sufficiently independent and, in particular, that one or more of the largest cloud providers has significant influence over the standards setting process. This could result in the standards benefitting certain cloud providers, to the detriment of others.

Consultation on potential remedies

- 9.46 Do you agree with our characterisation of common standards in cloud services and interfaces, as set out in Table 9.1 and, if not, why do you disagree?
- 9.47 Do you agree that common standards and standardisation in general are more appropriate for IaaS, ancillary services and tools and interfaces (APIs) than for more abstracted types of PaaS services?
- 9.48 What are the benefits and harms of introducing common standards for IaaS, ancillary services and tools and APIs?
- 9.49 What are the benefits in having common standards for cloud services where there is more abstraction?
- 9.50 Which standards setting bodies have sufficient independence and could set common standards for one or more of the types of cloud service or interfaces?
- 9.51 Should the standards apply to all cloud providers that offer a relevant cloud service or should standards only apply to the largest cloud providers?

Potential remedies that use principles-based requirements

- 9.52 Instead of implementing specific technical standards to achieve standardisation, we could require cloud providers to comply with a set of principles.
- 9.53 A principles-based remedy could also address the design of cloud services and/or the interfaces that customers, ISVs and other parties use to access or integrate with those services.

Stakeholder views

9.54 An ISV suggested requiring the large cloud providers to increase the degree of standardisation through the use of broad principles-based obligations.³⁸²

Design considerations

- 9.55 A principles-based approach to standard setting would require cloud providers to:
 - (a) achieve a stated outcome, for example, cloud providers must allow for comparability between bills raised by different providers; or
 - (b) take certain actions to achieve an outcome, for example, cloud providers should include certain headings on their bills to ensure comparability between bills from different cloud providers.
- 9.56 A principles-based approach could allow cloud providers greater freedom on how they comply. The level of freedom could vary depending on how tightly the principle is defined.
- 9.57 The principles could be applied to the largest cloud providers or to all cloud providers.
- 9.58 We would need to monitor the compliance of the cloud providers and take appropriate action in cases of non-compliance. Appropriate action could involve moving to a standards-based approach or taking enforcement action.

Potential impact

- 9.59 Principles-based requirements tend to be a less intrusive form of regulation, setting the direction or outcome, but giving cloud providers scope to decide how they comply.
- 9.60 A principles-based approach places high importance on and requires the involvement of monitoring and enforcement teams. As principles are less prescriptive than rules/standards, there is a need for a greater degree of scrutiny and assessment during monitoring and any enforcement processes.

Potential for unintended consequences

9.61 A potential drawback of a principles-based approach is that unless the principles are well defined there is a greater risk of misunderstanding and/or

circumvention compared to more tightly defined requirements. It may be possible to mitigate this risk by issuing detailed guidance or by iterating the principle or using a rule.

Questions for consultation

- 9.62 Is it preferable to impose broader principles-based requirements on cloud providers, or more prescriptive rules/common standards?
- 9.63 What broad principles should cloud providers be required to comply with, if we pursued a principles-based approach?
- 9.64 Should all cloud providers be required to comply with a principles-based approach or only the largest cloud providers?

Potential remedy to improve the interoperability of cloud services through the use of abstraction layers

- 9.65 In section 8 of this paper, we comment on customers' use of abstraction layers to abstract differences in the functionality between cloud providers, allowing customers to use cloud services across multiple clouds.
- 9.66 This potential remedy requires cloud providers to provide or support the provision of abstraction layers that automate or simplify the operation of the cloud technologies that sit below them in the cloud stack, allowing customers to centrally manage and use multiple clouds through a single standard interface. Given that there are existing abstraction layer products, we are considering whether the potential remedy should seek to improve the development, uptake and/or effect of existing abstraction layers for the purpose of improving customers' ability to switch and multi-cloud, or whether there may be alternative approaches such as requiring the creation of new abstraction layers.³⁸³
- 9.67 We understand that some customers use 'platform engineering' to develop so-called internal developer platforms. These platforms allow customers to abstract some aspects of the public cloud to assist the operation of their internal software development teams who use the public cloud.³⁸⁴ These platforms can also help reduce the potential for vendor lock-in.³⁸⁵ Through this potential remedy we would aim to ensure that the cloud providers take steps to facilitate the development of this type of and similar abstraction solutions.

³⁸³ See 'Questions for Consultation' starting at paragraph 9.81 below for more information.

³⁸⁴ 'What is Platform Engineering? – Pulimi', accessed 17 May 2024.

³⁸⁵ 'What is platform engineering? – Red Hat Blog', accessed 17 May 2024.

Stakeholder views

- 9.68 Academic research has proposed a standard 'compatibility layer' which could potentially help overcome some of the technical challenges identified in this working paper.³⁸⁶
- 9.69 Other academic research has developed abstraction layers over specific types of cloud infrastructure service, for example:
 - (a) Baarzi et al. prototyped a similar abstraction layer specifically for a type of cloud infrastructure service known as serverless functions, which in some applications can replace the use of virtual machines. This research states that characteristics of serverless functions make them uniquely suited to such an abstraction layer, but that the economic viability of providing such a layer may be a concern.³⁸⁷
 - (b) Elango et al. developed what they called a 'multi-cloud storage broker' that implements an API for object services, such as AW S3 and Azure Blob Storage, that can be used uniformly across a range of storage providers.³⁸⁸
- 9.70 UKCTA said that it sees value in industry, users and other stakeholders exploring ways to improve interoperability and portability, through market initiatives or otherwise.³⁸⁹

Design considerations

- 9.71 An abstraction layer would allow customers to use cloud services on third party clouds without the need for adapters or other tools.
- 9.72 The abstraction layer could be provided by a cloud provider or by an ISV.
- 9.73 We would be concerned if the cost acted as a barrier to customer uptake of abstraction layers. If we found this to be the case, we could require cloud providers to provide or support abstraction layers for free.
- 9.74 It may be appropriate to limit the scope of the potential remedy to specific services, for example foundational laaS services, such as compute and storage, or to all laaS services.

 ³⁸⁸ Elango et al. (2018), 'An Ontology-Based Architecture for an Adaptable Cloud Storage Broker', Advances in Service-Oriented and Cloud Computing ESOCC '17), pages 86-101.
³⁸⁹ UKCTA Response Cloud_Market_Review_Proposal.pdf (publishing.service.gov.uk).

³⁸⁶ Stoica, I and Shenker, S (2021), 'From Cloud Computing to Sky Computing', Proceedings of the Workshop on Hot Topics in Operating Systems HotOS '21), pages 26-32.

³⁸⁷ Baarzi, AF et al. (2021), 'On Merits and Viability of Multi-Cloud Serverless', Proceedings of the ACM Symposium on Cloud Computing (SoCC '21), pages 600-608.

9.75 The potential remedy could be applied to a subset of IaaS providers. The potential remedy is unlikely to be applied to all IaaS providers, as it could disproportionately increase costs for smaller IaaS providers, who already have greater incentives to make their services more interoperable.

Potential impact

- 9.76 An abstraction layer would facilitate integration and increase interoperability between cloud providers by abstracting underlying differences in functionality between cloud services on different clouds. This could make it simpler and less costly for customers to use cloud services which best meet their needs, across multiple public clouds.
- 9.77 Requiring an abstraction layer could lead to greater standardisation of IaaS functionality, as cloud providers may coalesce around similar solutions to achieve the required outcome.

Potential for unintended consequences

- 9.78 Requiring an abstraction layer could lead to reduced innovation, as it would reduce perceived differences between cloud provider services. In certain circumstances, the underlying difference in functionality may be beneficial to customers, if that difference leads to better performing products/services, as providers are better able to introduce new functionality that has non-equivalent outputs (at least in the short-term).
- 9.79 There is a risk that requiring cloud providers to offer solutions that assist customers in using multiple public clouds could allow cloud providers to extend the reach of their ecosystems; increasing the potential for customer lock-in.
- 9.80 If cloud providers were required to provide or support abstraction layers for free, they may look to recoup the cost of the abstraction layer by increasing the prices of other cloud services.

Questions for consultation

- 9.81 To what extent do the products already offered by the cloud providers, such as Azure Arc and Google Anthos, act as an abstraction layer and allow customers to operate across multiple public clouds?
- 9.82 To what extent do IaC products already offered by ISVs, such as Terraform (by HashiCorp) or Pulumi, act as an abstraction layer and allow customer to operate across multiple public clouds?

- 9.83 To what extent could cloud providers extend the reach of their ecosystems by offering abstraction layers and would this increase the potential for customer lock-in? If so, how could this risk be mitigated?
- 9.84 To what extent does abstraction also require underlying standardisation?
- 9.85 Would a potential requirement for cloud providers to offer abstraction layers benefit or harm ISVs who offer the same or similar solutions?
- 9.86 What action(s) could we take to increase the uptake of existing abstraction products offered by ISVs?
- 9.87 What action(s) could we take to increase or improve competition to develop abstraction layers?
- 9.88 Should we require cloud providers to offer abstraction layers for a subset of laaS services for free, and, if so, which laaS services should be in scope?
- 9.89 Under what circumstances would the potential remedy no longer be required and should be allowed to lapse?

Potential remedies to increase interconnectivity and reduce latency

- 9.90 Some customers said that latency can be a challenge in integrating multiple public clouds, particularly when the integration involves workloads that require real-time or near-real-time transfers of data.
- 9.91 In this section we consider potential remedies that seek to address challenges with latency that inhibit customers integrating multiple public clouds. We recognise that these potential remedies have particular risks, including potential implications for incentives to invest in data centres and cloud infrastructure more generally.
- 9.92 While we welcome views on these potential remedies, we are not currently minded to prioritise them in this investigation. We also welcome views on alternative ways to reduce latency between cloud providers and, by doing so, increase the potential for customers integrating multiple public clouds.

Stakeholder views

9.93 Company A suggested increasing interconnectivity by connecting the data centres of the largest cloud providers to other cloud providers' data centres,

as this would help address key concerns around technical barriers to interoperability and portability.³⁹⁰

9.94 Company A also suggested that cloud providers should provide choice to customers over interconnection mechanisms (eg private peering,³⁹¹ public peering³⁹² etc).³⁹³

Potential remedy that involves connecting third party data centres

- 9.95 A data centre provider told us that, in the UK, there are concentrations of data centre in Slough, London and Manchester.³⁹⁴ At the moment data centres operated by different cloud providers are generally connected using the public internet, meaning that latency is high because data must travel through one or more Internet Exchange Points (IXPs).
- 9.96 This potential remedy would involve building direct fibre lines between all the data centres of different cloud providers in a data centre hub.

Design considerations

- 9.97 We would need to establish the geographical boundaries of the data centre hub. We could consider the location of data centres currently used by cloud providers and cloud providers' current regions and availability zones when deciding on the boundaries of a data centre hub.
- 9.98 Any data centres located in the hub that are owned or used by a cloud provider would be connected using direct fibre lines.
- 9.99 The following points are also of relevance to the design of this potential remedy:
 - (a) the cost of the direct fibre lines may need to be shared across relevant cloud providers;
 - (b) there may be the need for joint or independent oversight and/or maintenance; and
 - (c) an independent body may be required to identify and designate new data centre hubs in other locations.

³⁹⁰ Company A's response to the Issues Statement, 17 October 2023.

³⁹¹ Private peering is the direct connection of two networks using a point-to-point connection.

³⁹² Public peering is the interconnection of many different networks and typically occurs at internet exchange points.

³⁹³ Company A's response to the Issues Statement, 17 October 2023.

³⁹⁴ Note of meeting with [>].

Potential impact

9.100 Transfers of data between data centres within a hub would benefit from lower latency. This could increase the potential for customers using services on multiple clouds.

Potential for unintended consequences

- 9.101 This potential remedy could disincentivise investment in new data centres in the UK, reducing the supply of data centre infrastructure.
- 9.102 The potential remedy could also lead to a concentration of data centres in the data centre hubs. This could increase demand for land and energy in these locations, potentially leading to higher land prices and issues with the supply of energy.
- 9.103 Data centres located outside of the hubs and areas without a hub, may not benefit from lower latency, placing these data centres/areas and the customers they serve at a disadvantage.
- 9.104 The cost of building the direct connections to connect the data centres would fall on the cloud providers, who may in turn attempt to recoup that cost through higher prices.

Potential remedy that requires cloud providers to make data centre space available for other cloud providers

9.105 We have seen evidence of partnerships between some cloud providers, such as Oracle leasing space in Microsoft's data centres³⁹⁵ and an agreement between Microsoft and Nvidia to deploy Nvidia GPUs in Microsoft data centres.³⁹⁶ This potential remedy could allow for these types of agreement to be expanded across the industry.

Design considerations

- 9.106 Cloud providers could be required to make space available in their data centres to other cloud providers on fair, reasonable, and non-discriminatory (FRAND) terms.
- 9.107 The space that a cloud provider would need to make available to other providers in one of its data centres could be capped at a minimum level

³⁹⁵ 'Microsoft and Oracle Expand Partnership to Deliver Oracle Database Services on Oracle Cloud Infrastructure in Microsoft Azure', accessed 23 May 2024.

³⁹⁶ 'NVIDIA Teams With Microsoft to Build Massive Cloud AI Computer | NVIDIA Newsroom', accessed 23 May 2024.

specified as a percentage of the data centre's total capacity. Above the cap the cloud provider would have discretion whether to make further space available.

- 9.108 The potential remedy could apply to the largest cloud providers or to all cloud providers.
- 9.109 An arbitration or appeal mechanism may be required for situations where cloud providers cannot agree on what constitutes FRAND terms.

Potential impact

9.110 Customers would benefit from lower latency as the physical distance between cloud providers' servers would be much reduced. This could increase the potential for customers using services on multiple clouds.

Potential for unintended consequences

- 9.111 This potential remedy could disincentivise investment in new data centres in the UK, reducing the supply of data centre infrastructure.
- 9.112 Requiring cloud providers to offer data centre space to their competitors on FRAND terms, could also have unintended consequences and practical difficulties, such as:
 - (a) cloud providers forcing their competitors to make space available in desirable locations;
 - (b) cloud providers not having the capacity they initially planned for in certain locations;
 - (c) situations where demand for space in a data centre exceeds the available space;
 - (d) situations where cloud providers sell or exit a data centre and require all other cloud providers who use space in the data centre to exit with little or no notice; and
 - (e) issues around security and access to third party data centres.

Remedies requiring cloud providers to be more transparent about the interoperability of their cloud services

9.113 In this section we consider potential remedies that require cloud providers to be more transparent about the interoperability of their cloud services.

- 9.114 By increasing transparency around interoperability it may reduce the potential for customers choosing services that lock them into a cloud provider.
- 9.115 We are considering the following potential remedies to improve transparency:
- 9.116 Requiring cloud providers to publish documentation on:
 - (a) the interoperability of each service that includes a clear explanation of the compatibility with third party cloud services; and
 - (b) how customers would migrate away from or exit the cloud service.
- 9.117 Requiring cloud providers to publish information on forthcoming major changes to their underlying cloud services.

Stakeholder views

9.118 Company A suggested that large cloud providers should be more transparent about the interoperability of their cloud services.³⁹⁷

Remedy requiring cloud providers to publish documentation on the interoperability of cloud services and the ability to migrate away from cloud services

Design considerations

- 9.119 Our current thinking is that cloud providers would be required to publish the documentation on the interoperability of their services in a single, easily discoverable and accessible place.
- 9.120 The potential remedy could be limited to a subset of cloud services, for example, the services that are used the most or it could apply to all cloud services.
- 9.121 Any requirements for increased transparency could apply to the largest cloud providers, or to all cloud providers.

Potential impact

9.122 Customers would be better informed on the interoperability of cloud services, allowing them to make more informed decisions. This could reduce the potential for lock-in, as customers could better design their cloud architecture

³⁹⁷ Company A's response to the Issues Statement, 17 October 2023.

in a way that allows them to use multiple clouds and access cloud services which best suit their needs.

Potential for unintended consequences

- 9.123 The effect of a requirement to publish details on the interoperability of cloud services could increase over time as cloud services become more numerous and complex, so that it might become more onerous and costly for cloud providers to comply.
- 9.124 There is also the possibility that if too much information is published or the information published is too detailed or technically complex, then some customers, and in particular smaller customers, may not have the resources needed to properly assess or act on the information.

Questions for consultation

- 9.125 Should the potential remedy only apply to the largest cloud providers or to all cloud providers?
- 9.126 Which cloud services should this potential remedy apply to?
- 9.127 Under what circumstances would the potential remedy no longer be required and allowed to lapse?

Remedy requiring cloud providers to give notice and publish details of upcoming material updates to cloud services

Design considerations

- 9.128 Cloud providers would be required to publish details of any upcoming major updates to their cloud services in a single, easily discoverable and accessible place. In particular, this remedy could allow ISVs who build on those cloud services to pass on relevant benefits to customers with minimal delay. Cloud providers would need to give sufficient notice, for example, a minimum of 30 days for any upcoming major updates to a cloud service.
- 9.129 In cases of emergency, cloud providers would be allowed to process major updates quicker. For example, if a cloud provider identified an issue with the security of one of its services.
- 9.130 The potential remedy could be limited to a subset of cloud services, for example, the services that are used the most or it could apply to all cloud services.

9.131 Any requirements for increased transparency could be targeted at the largest cloud providers or apply to all cloud providers.

Potential impact

9.132 Stakeholders, particularly ISVs, would also be better informed about major changes to cloud services, meaning that they are able to process updates to their services on a timely basis. This may allow them to provide a better service to customers and to better compete with the larger cloud providers.

Potential for unintended consequences

- 9.133 Cloud providers may be delayed in processing material updates to services, meaning that customers may be delayed in receiving the benefit associated with the update.
- 9.134 The requirement to publish material updates to cloud services could increase the regulatory burden on cloud providers and may increase their costs.

Questions for consultation

- 9.135 What constitutes a material update to a cloud service?
- 9.136 Do cloud providers already give sufficient notice of material updates to their services?³⁹⁸ If not, how much notice should cloud providers give stakeholders of a material update to a cloud service?
- 9.137 What are the circumstances that would constitute an emergency, where cloud providers would be allowed to process a material update to a cloud service without giving notice?
- 9.138 Should the potential remedy only apply to the largest cloud providers or to all cloud providers?
- 9.139 Which cloud services should this potential remedy apply to?
- 9.140 Under what circumstances would the potential remedy no longer be required and allowed to lapse?

³⁹⁸ For example, we understand that both AWS and Microsoft publish details of releases and updates to their cloud services via publicly-available feeds 'Subscribe to AWS Daily Feature Updates via Amazon SNS', accessed 21 May 2024, and 'Azure updates – Azure Documentation', accessed 21 May 2024).

Remedies to improve skills

- 9.141 In section 7 of this paper, we note that the level of technical differentiation between the various public clouds affects customers being able to access a workforce with relevant skills and that this challenge may increase the cost to customers of operating across multiple cloud environments or switching between clouds.
- 9.142 Any reduction in technical differentiation between public clouds from our other potential remedies may reduce the need for a remedy specific to skills.
- 9.143 In the rest of this section we consider potential remedies to improve skills of cloud engineers and IT staff in the UK. These potential remedies assume that there continues to be some technical differentiation between cloud providers and that the technical differentiation requires remedial action.

Require cloud providers to make training and education courses cloudagnostic

9.144 This potential remedy would seek to increase the ability of technical staff to work across multiple clouds by requiring a portion of any training provided on cloud services to be cloud-agnostic.

Design considerations

9.145 Our current thinking is that the potential remedy could:

- (a) apply to any cloud related training offered by cloud providers; and
- (b) require a minimum amount of the material covered to be cloud-agnostic.

Potential impact

9.146 The potential remedy would increase the ability of individuals to work across cloud environments.

Potential for unintended consequences

- 9.147 The potential remedy might make any training or education course less useful, as some of the training may not be specific to an individual's role or circumstances.
- 9.148 It may also limit the ability of individuals to specialise in one area, as any training would likely be more general.

Questions for consultation

- 9.149 What constitutes cloud-agnostic training?
- 9.150 What percentage of training courses should be cloud-agnostic?
- 9.151 Are there any other potential remedies that involve improving skills or making training more cloud-agnostic?

Summary of potential remedies and invitation to comment

- 9.152 As explained above, we have set out our early views on the approach and design of the potential remedies that we discussed in our issues statement. In particular we have identified potential remedial approaches which would seek to address the service and non-service related technical challenges discussed in this working paper.
- 9.153 Our consideration of potential remedies is ongoing. We will consider further any cross-cutting remedy design elements in a later working paper on potential remedies.