Appendix W: Remedies appendix

Introduction

W.1 This appendix describes the potential remedies that we have considered during this investigation but have provisionally decided not to pursue through our remedy-making powers under the Act. These address the AECs we have provisionally found relating to:

(a) Technical barriers;

(b) Egress fees; and

(c) Microsoft's licensing practices.

W.2 This appendix should be read in conjunction with Chapter 9 of the provisional findings report which sets out our proposed remedies, as:

(a) Remedy 1: a recommendation to the CMA Board to prioritise commencing an SMS investigation of AWS' digital activities in respect of cloud services, and if an SMS designation is made to consider imposing appropriate interventions such as those identified in this report; and

(b) Remedy 2: a recommendation to the CMA Board to prioritise commencing an SMS investigation of Microsoft's digital activities in respect of cloud services, and if an SMS designation is made to consider imposing appropriate interventions such as those identified in this report.

W.3 The reasoning for this, including why the design of the digital competition regime powers are better suited to addressing the concerns we have identified than the powers directly available to us in this market investigation, is included in that chapter.

W.4 We note that during the course of our investigation, we received representations regarding the implications of potential remedies, in particular in relation to the effects on implementation costs, innovation and customer choice.[1] As part of our

[1] In particular, see: AWS' response to the Technical barriers working paper dated 31 July 2024, paragraph 76; Google's response to the Technical barriers working paper dated 27 June 2024, paragraph 28; Submissions to the CMA [✂]; AWS' response to the Egress fees working paper, paragraphs 14-19 and 28; Microsoft's response to the Competitive landscape, Committed spend agreements and Egress fees working papers, paragraphs 9, 83, 97-99; Google's response to Egress fees working paper, paragraph 57 and Annex responses (c) and (h).

consideration of potential remedies we considered these submissions and focused on potential remedies that would avoid unnecessary costs and restrictions.

Technical barriers

W.5 In this section, we set out our views on potential remedies to the technical barriers we have found. We have structured the section as follows:

(a) first, we provide a description of these potential remedies.

(b) second, we summarise stakeholder views on potential remedies.

(c) third, we set out an analysis of the effectiveness of the potential remedies to technical barriers.

(d) finally, we include our views on remedies to technical barriers that could be implemented through a market investigation order.

Description of potential remedies

W.6 We have considered eight potential remedies to address the AEC we have provisionally found relating to technical barriers:[2]

(a) requiring cloud providers to adopt common standards:

(i) in IaaS (Potential remedy 1);

(ii) in PaaS (Potential remedy 2);

(iii) for ancillaries (Potential remedy 3); and

(iv) for interfaces (Potential remedy 4).

(b) requiring cloud providers to offer abstraction layers (Potential remedy 5);

(c) increasing interconnectivity and reducing latency through connecting third party data centres or requiring cloud providers to make space available in their data centres (Potential remedy 6);

(d) increasing transparency around the interoperability of cloud services (Potential remedy 7); and

[2] This list includes the potential remedies that were discussed in the Technical barriers working paper and concerned: increasing the degree of standardisation of cloud services and/or interfaces, improve the interoperability of cloud services, increase interconnectivity and reduce latency, increase transparency and improve the portability of skills.

(e) requiring cloud providers to make training and education courses cloud agnostic (Potential remedy 8).

Stakeholder views

W.7 We received various submissions on the potential remedies considered in our working paper on technical barriers.[3] We have grouped the responses by topic.

W.8 AWS submitted that the potential interventions considered will not resolve the inherent technical barriers and risk harming customer choice and innovation.[4]

W.9 Google submitted that market-wide remedies are unnecessary, not proportionate and complex in a fast-moving market with new emerging technologies, and could lead to unintended distortions to market outcomes, including by potentially hampering innovation.[5] Instead, Google noted that any remedy should be limited to addressing the provider-specific technical barrier(s) that customers have consistently identified - ie the artificial restrictions that Microsoft imposes that limit interoperability between Active Directory and third party IAM solutions.[6]

W.10 Microsoft and IBM suggested a role for the open-source community in remedies:

(a) Microsoft submitted that it strongly believes that an intervention to address technical barriers is more likely to succeed, and less likely to lead to unintended consequences, if it harnesses the existing efforts of the open-source community. It said that the open-source community is best placed to understand what would (and what would not) work on these complex and technical issues, and gave four specific examples of ways the CMA could promote and empower these foundations and open-source software. These included:

(i) mandatory membership of the Cloud Native Computing Foundation (CNCF) for cloud providers;

(ii) funding contributions beyond membership fees, to ensure that the Linux Foundation[7]/CNCF has the resources to keep up with the market;

[3] The potential remedies in the Technical barriers working paper concerned: increasing the degree of standardisation of cloud services and/or interfaces, improve the interoperability of cloud services, increase interconnectivity and reduce latency, increase transparency and improve the portability of skills.
[4] AWS' response to the Updated issues statement and working papers dated 23 May 2024 and 6 June 2024, paragraph 69.
[5] Google's response to the Technical barriers working paper dated 6 June 2024, paragraph 28.
[6] Google's response to the Technical barriers working paper dated 6 June 2024, paragraph 29.
[7] The Linux Foundation is the parent of CNCF.

(iii) contributions to operations, corporate governance, and technical governance, such as via the CNCF's Technical Oversight committee; and

(iv) a commitment that support for open source 'mitigations' will be conformant, where a conformance certification programme exists.[8]

(b) IBM submitted that it considers that the best way to ensure appropriate governance for standards would be to rely on the Linux Foundation.[9]

W.11 Various stakeholders commented on mandatory technical standards:

(a) AWS submitted that mandatory regulator-enforced standards are, in its view, incompatible with dynamic and innovative industries such as the IT sector.[10]

(b) AWS also submitted that even if technical standards encapsulate the optimal solutions at the time they are set, they will likely not be optimal solutions for future problems.[11]

(c) AWS also said that stifling the development of innovative proprietary technologies in the name of interoperability or portability would harm competition by limiting the ability of, 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.[12]

(d) Google submitted that it does not think it is appropriate, or practical, for any local regulator to have oversight over common standards. Google also noted that it does not consider that there is currently any relevant body either in the UK or globally, with sufficient independence or the necessary degree of specialist knowledge to set common standards for the cloud industry across a broad range of diversified cloud products and services.[13]

(e) [✂] said that in areas where open-source standards exist, [✂] would be cautiously supportive of a requirement to follow such standards. In areas

[8] Microsoft's submission on the CMA's conceptual remedies framework dated 23 August 2023, paragraph 7.
[9] IBM's response to the Technical barriers working paper dated 6 June 2024, page 4.
[10] AWS' response to the Updated issues statement and working papers dated 23 May 2024 and 6 June 2024, paragraph 68.
[11] AWS' response to the Updated issues statement and working papers dated 23 May 2024 and 6 June 2024, paragraph 68.
[12] AWS' response to CMA's information request [✂].
[13] Google's response to the Technical barriers working paper dated 6 June 2024, Annex 1.

where no such standards exist, caution is needed. In particular, [✂] notes that mandating interoperability standards for PaaS would not only require cloud providers to adapt their offering to these standards but would also require some adaptation on the customer side, which could be costly in the short term.[14]

(f) IBM submitted that in cases where standards do not exist, the lack of open standards is not due to a lack of willingness but due to technical complexity and high costs. [✂].[15]

(g) CCIA noted that standardisation can enhance competition to the extent products are then closer to commodities and easier to substitute for one another. However, it also referenced a long-standing critique that compulsory standardisation could undermine more meaningful dynamic competition by impeding differentiation in the market and suggested that if we opt for standardisation that we work with established standards, rather than develop new standards.[16]

(h) Vodafone submitted that continued innovation should be supported, at any layer of the cloud stack. Vodafone also noted that for mature technologies, standards could help since there is less service innovation or change – IaaS primarily offers compute, storage and networking which can all be defined as code or by calling an API. Each cloud provider today uses proprietary 'language' to drive this and there is no common API.[17]

(i) a stakeholder told us that standardising identity management – which it said could, for example, allow a customer to create one account in OVHcloud but request resources from AWS – is a change that would significantly foster interoperability. However, it also said that the commercial aspects of this could be a challenge in practice.[18]

(j) an academic submitted that strict technical standards could hinder innovation.[19]

W.12 Microsoft and the CCIA argued against a principles-based approach to remedying technical barriers:

(a) Microsoft submitted that a principles-based approach may be even worse than mandatory standards, as a principles-based approach requires an arbiter to determine whether market participants have adhered to the

[14] [✂] submission to the CMA [✂].
[15] IBM's submission to the CMA.
[16] CCIA's response to the Technical barriers working paper dated 06 June 2024, page 2.
[17] Vodafone's response to the working papers dated 23 May 2024 and 06 June 2024.
[18] [✂] submission to the CMA [✂].
[19] R. Parisi, The Cloud Services Markets' Competitive Landscape: A contribution to the Competition and Markets Authority, page 14.

principles, which in turn have to interpret these principles in day-to-day and strategic business decisions. Microsoft stated that this introduces significant uncertainty, and therefore also functions as a brake on innovation.[20]

(b) CCIA submitted that with principles-based approaches a company is faced with an expectation that it feels it is unable to meet and is expected to invent a solution. This is particularly the case for interoperability where an effective solution will often depend on other market participants.[21]

W.13 Microsoft and [✂] commented on open APIs:

(a) Microsoft said that cloud providers are incentivised to make available APIs, such as those used by ISVs to develop abstraction layers, and do so already. It said that ensuring that they remain accessible is a worthwhile in-market solution that the CMA should consider.[22]

(b) [✂] said that publishing open APIs is key to allowing interoperability, and in particular for a third party provider to develop efficient ancillary services for customers. But APIs also need to be as stable as possible (in terms of frequency and advance notice of updates, and commitments to maintain open access) so that providers can have sufficient confidence to justify incurring the necessary development costs.[23]

(c) [✂] said that a requirement to publish open and stable APIs could be limited to largest providers without too many adverse consequences.[24]

W.14 Some stakeholders commented on Identity and Access Management:

(a) Google said that Microsoft should provide Active Directory Interoperability information sufficient to allow competing cloud providers to integrate with Active Directory.

(b) some academic researchers (Professor Ion Stoica, Professor Scott Shenker, and Assistant Professor Aurojit Panda) said that it is not obvious why other cloud providers would adopt AWS Cedar. [25]

W.15 Some stakeholders commented on improving transparency:

(a) Google submitted that, in its view, there is already a high degree of transparency in the market and that it does not consider that increasing the

[20] Microsoft's response to the Technical barriers working paper dated 06 June 2024, paragraph 67.
[21] CCIA's response to the Technical barriers working paper dated 06 June 2024, page 3.
[22] Microsoft's submission on the CMA's conceptual remedies framework dated 23 August 2023, paragraph 2.
[23] [✂] submission to the CMA [✂].
[24] [✂] submission to the CMA [✂].
[25] AWS Cedar is an open-source policy language and authorisation engine for fine-grained permissions management. Note of meeting with [✂].

amount of information available to customers would address the underlying barriers to switching or multi-cloud.[26]

(b) IBM submitted that increased transparency and better customer information could go a long way to improving market conditions in the short term, especially regarding the publication of open APIs/SDKs.[27] However IBM added that requiring all CSPs to describe eg, how customers can migrate away from their cloud may however not be efficient (customers need automation and tools more than information to migrate) and risks imposing a disproportionate burden on smaller providers.[28]

(c) a customer said it welcomes remedies such as increased transparency and the removal of technical barriers to switching as these are most likely to positively impact competition and consumer choice.[29]

W.16 Google said that if a provider decides to update its services, any third party service workarounds have to be updated to ensure ongoing interoperability. Google suggests that the provider making the change gives 12 months' notice of a material change and particularly, any upcoming discontinuation of services or related material functionality for which they do not offer a replacement similar service or functionality, to allow other industry players time to respond and to ensure continued interoperability with their services. Google noted that increasing notice would not address the underlying barriers to switching or multi-cloud.[30]

Analysis of the potential remedies for technical barriers

W.17 In this section, we set out an analysis of each the potential remedies. We discuss the design considerations before assessing their effectiveness.

Standardisation remedies (Potential remedies 1 to 4)

Description of remedy and intended effect

W.18 The purpose of standardisation remedies in the context of cloud services would be to standardise one or more aspects of the service to improve interoperability, which in turn should allow customers to better and more easily switch and/or use multi-cloud.

[26] Google's response to the Technical barriers working paper dated 6 June 2024, Annex 1.
[27] Software Development Kit.
[28] IBM's response to the Technical barriers working paper dated 6 June 2024, page 2.
[29] [✂] submission to the CMA [✂].
[30] Google's response to the Technical barriers working paper dated 6 June 2024, Annex 1.

Design considerations

W.19 Below we discuss the key design, implementation and governance considerations for a standardisation remedy to technical barriers:

(a) which cloud providers are in scope?

(b) which cloud services are in scope?

(c) what standard(s) to use?

(d) how is the standard developed and/or maintained?

(e) is the standard voluntary or mandatory?

(f) how is monitoring and enforcement conducted effectively?

W.20 The specific design choices have implications for the risk profile of the remedy, in particular with regard to (i) specification risks, where it may be difficult to specify the operations of the remedy in sufficient detail, (ii) distortion risks, where detriments may arise from overriding market signals, and (iii) monitoring and enforcement risks, where determining compliance may be difficult and risks undermining the effectiveness of the remedy.

Cloud providers in scope

W.21 A remedy requiring the adoption of common standards could:

(a) include all cloud providers;

(b) set a minimum size threshold (eg set by reference to revenue) and include all cloud providers above that threshold; or

(c) be limited to cloud providers which have significant market power.

W.22 We consider that there would be benefit in targeting the remedy at a small number of larger providers. This is because:

(a) the cloud services market is concentrated, for example AWS and Microsoft have a combined market share (IaaS and PaaS) of 60-70% (and 80-90% of IaaS market). Therefore, the majority of customers in the cloud services market would benefit directly from a remedy that covered the two largest suppliers in particular. It could also apply to a small number of suppliers above a particular threshold that account for the remaining proportion of the cloud services markets.

(b) larger firms have a greater incentive to maintain or increase technical barriers to switching and multi-cloud, in order to make it harder for their larger existing customer bases to switch away.

(c) conversely, smaller providers have a greater incentive to reduce barriers, including by voluntarily adopting standards, particularly where this might provide them with access to large customer bases (such as those currently held by AWS and Microsoft). For example, Google,[31] Oracle,[32] Civo,[33] IBM[34] and OVHcloud[35] all developed AWS S3-compatible APIs to assist in moving data.

W.23 There are also practical benefits of having fewer firms in scope of these remedies, as it would reduce complexity and associated levels of resource required for implementation, monitoring and enforcement.

W.24 We note that there is a distortion risk associated with narrowing the number of cloud providers in scope. In particular, there is a risk that these providers could exert excessive control over the design or maintenance of a standard, such that it better suits their own needs than those of other suppliers (eg better integrating into their wider product base). Therefore, the potential remedy would need to include a robust governance structure, both initially and on an ongoing basis, to mitigate this risk.

Cloud services in scope

W.25 When designing the remedy, it is necessary to specify which services are in scope. This may require considering the scale of harm arising from the absence of an existing lack of standard for a given cloud service or category of cloud services, as well as the expected costs of developing, implementing and maintaining such a standard.

W.26 One potential cost of requiring common standards is that it has the potential to reduce or limit the scope for differentiation on certain parameters, which in turn could suppress incentives to innovate. We consider that the potential impact would vary depending on the extent of innovation in the relevant cloud service(s).

W.27 We also consider that the standardisation of APIs may increase the interoperability of a cloud service, while continuing to allow for some functional differentiation between cloud providers. The implication being that standardising interfaces may have a lesser impact on innovation than standardising the underlying features.

---

[31] Interoperability with other storage providers - Cloud Storage - Google Cloud accessed 26 November 2024.
[32] Object Storage Amazon S3 Compatibility API, accessed 26 November 2024.
[33] Data Management with Civo Object Stores, accessed 26 November 2024.
[34] IBM Cloud Object Storage S3 API - IBM Cloud API Docs, accessed 26 November 2024.
[35] Object Storage - FAQ - OVHcloud, accessed 26 November 2024.

W.28 In summary, we consider that the potential impact of standardisation on innovation varies between different cloud services and between the features of cloud services and APIs. It is our provisional view that standardising APIs, IaaS and ancillary services generally has lower associated distortion risks, while standardising differentiated PaaS services has greater associated distortion risks. We also note that for any one cloud service, the impact of standardisation on innovation has the potential to change over time. Therefore, unless the remedy is able to adjust to these changes, there is the potential to dampen innovation in certain cloud services.

What standard(s) to use

W.29 One of the main design considerations is identifying and specifying the technical standard to apply, for example:

(a) a common open-source standard may exist but may have limited uptake;

(b) a generally accepted standard may exist, but is controlled by a single supplier; or

(c) no common standard exists, and it may need to be developed.

W.30 The standard that is chosen could favour integrations with one cloud over another, creating distortions. For example, if a common standard was set so that it aligned with a proprietary technology used by one cloud provider, it could give that cloud provider undue influence over the cloud services in scope. In these cases, it may be necessary to establish an independent oversight mechanism for the development and/or maintenance of the standard.

W.31 Furthermore, for cloud services where there is more innovation and where the services are still developing, there is a risk that a regulatory intervention could suppress natural developments in the market. A remedy that introduces a standard could override market signals by forcing suppliers to use a suboptimal standard, and in turn prevent a superior standard from being adopted.

How is the standard developed and/or maintained

W.32 Developing common standards requires a degree of coordination between the relevant companies, which typically requires a standards setting body to be engaged to oversee the development, implementation, and maintenance of any standard.

W.33 There are a number of key considerations for an effective standard setting body, in particular:[36]

(a) independence: the standard setting body would need to be sufficiently independent from the cloud providers to reduce the scope for undue influence to be exerted on the process by one or more cloud providers.

(b) capability: the standard setting body would need to have sufficient expertise to oversee the development, implementation and ongoing governance required to iterate the standard.

(c) resourcing/funding: the standard setting body would need to have sufficient resources and, in particular, sufficient funding to carry out its duties. This would not only need to be in place when the standard is developed, but also on an ongoing basis to mitigate the risk of the standard becoming outdated and ineffective over time.

W.34 Microsoft and IBM have suggested that the Linux Foundation (potentially through the CNCF) could fulfil this role.[37] We recognise the positive contribution that open-source foundations such as the Linux Foundation have on the cloud services market and the expertise that they are able to harness. However, for a standardisation remedy to be effective when including an open-source foundation, we would need to ensure that:

(a) any project to develop the technical standard would be adopted and promoted by the open-source foundation;

(b) the open-source foundation has access to the requisite expertise through its community and this expertise could be called upon when required;

(c) governance structures are in place to mitigate the risk of capture by the larger companies; and

(d) a backstop existed to enforce standards, should the project stall or cloud providers decline to adopt the standard that had been developed.

W.35 We considered that including an open-source foundation as a standard setting body has associated risks. These foundations were not designed to oversee a CMA remedy, and their existing structures are unlikely to be naturally well suited to this task. For example, the CNCF does not have specific governance processes for its projects, instead allowing contributors to decide how a project should be governed, including how much influence / voting rights any one organisation can

[36] We note that these closely mirror Recommendation 4 of the Open Banking Lessons Learned Review which included key factors to consider where a remedy establishes a new entity or large and enduring CMA function.
[37] Microsoft's submission on the CMA's conceptual remedies framework dated 23 August 2023, paragraph 7; IBM's response to the Technical barriers working paper dated 6 June 2024, page 4.

have over the project.[38] Furthermore, we are aware that the responsibilities associated with our remedies may impinge on the foundation's wider aims and functions. Therefore, it is not clear that there are existing bodies that would be well suited to develop and maintain standards as part of a potential remedy.

W.36 In the absence of an appropriate existing standard setting body it may be necessary to establish a new, specialist body to oversee the development, implementation and maintenance of any standards. This would likely be complex and come with its own risks, particularly when defining the scope, purpose, status and funding of the entity, its proposed governance arrangements, accountability of different stakeholder groups, including the CMA, and overall decision making processes governing each of them.[39] Furthermore, the role of this body may need to change over time, for example with regard to the list of standards it is overseeing which could in turn have implications for the entity (eg the provision of funding may need to flex to reflect which cloud providers' services are within scope).

Voluntary vs mandatory standards

W.37 While we recognise that there may be some benefits to allowing cloud providers to implement standards via voluntary schemes, we consider that there are risks with this approach. We consider that there would be a need for a mandatory scheme to act as a backstop, should the voluntary scheme prove ineffective or should cloud providers attempt to frustrate the development and/or implementation of the voluntary scheme.

W.38 We also note that, even where a standard is developed and adopted voluntarily, there is still a risk that a subset of cloud providers could exert undue influence over the process. To mitigate this risk, the considerations discussed above are likely to remain relevant.

Monitoring and enforcement

W.39 There are monitoring and enforcement considerations that relate to the ongoing oversight of common standards.

W.40 Ongoing oversight would be required to monitor and maintain standards as the cloud services market changes. We expect that this ongoing oversight would need to be provided, at least in part, by the independent body discussed above.

W.41 We note that provisions would be required to give the independent body the ability to carry out this function, ideally without reliance on a cumbersome and/or slow

[38] Governance: Leadership Selection - CNCF Contributors last accessed on 23 October 2024.
[39] For example, see Recommendation 4 of the Open Banking Lessons Learned Review which includes key factors to consider where a remedy establishes a new entity or large and enduring CMA function.

enforcement mechanism (eg by placing obligations on suppliers to engage in particular ways with clearcut and easily enforceable requirements). If this is not included, and if the independent body was delayed in its decision making by having to defer all investigatory work and/or decisions to the CMA, it could result in higher monitoring and enforcement risk.

Effectiveness assessment

W.42 We consider that requiring cloud providers to adopt mandatory common standards through a market investigation order could, in principle, address some of the harms from technical barriers for customers when switching or using multiple clouds. However, in practice, there are likely to be material risks depending on the specific approach.

W.43 We assessed the effectiveness of mandatory standards, by considering the design considerations described above and applying them to the specific characteristics of IaaS, PaaS, ancillaries and interfaces, which we note in the chapter on technical barriers contribute to the AEC we have provisionally found. We set out our assessment under the following headings:

(a) expected impact on AEC and risk profile;

(b) monitoring compliance and enforcement;

(c) timescales; and

(d) interactions with other laws and regulations.

Expected impact on AEC and risk profile

W.44 In assessing the expected impact that potential remedies implementing common standards could have on the AEC we have provisionally found, and the associated risk profiles, we particularly considered:

(a) distortion risks for specific services;

(b) circumvention risks from cloud providers re-imposing barriers;

(c) the standards setting body; and

(d) the cloud providers in scope.

Distortion risks for specific services

W.45 As described above, the introduction of common standards could, in some circumstances, reduce the ability and/or incentive of cloud providers to innovate through improving and differentiating their services.

W.46 We consider that this risk is lower for more mature cloud services, such as IaaS and ancillary services, and APIs, than it is for newer and more innovative PaaS services, such as Function as a Service (FaaS).

W.47 The specific set of cloud services where the likely benefits of requiring a common standard exceed the distortion risks are difficult to discern at this stage and are also likely to change over time. We are also aware that technical mitigations have been developed, and new routes may emerge which could further affect this balance.

W.48 We have not been able to identify a mechanism by which we could specify in advance when the threshold for intervention would be met, and so a remedy that would contribute effectively to a comprehensive solution would likely require substantial ongoing monitoring and analysis, as well as allowing for a changing list of services within its scope.

Circumvention risks from cloud providers re-imposing barriers

W.49 There are numerous points of technical friction for customers when switching or operating across multiple clouds (see Chapter 5). If standards were introduced that increased interoperability and customers' ability to switch between clouds for some cloud services, it is possible that cloud providers, and particularly the largest cloud providers, would be able to reintroduce technical frictions elsewhere in their ecosystems. The concerns associated with circumvention are particularly acute in relation to AWS and Microsoft, given we have found them to have substantial market power.[40]

W.50 This risk is particularly relevant to standards imposed through a market investigation, given the need to specify the cloud services and interfaces that are in scope of any order and that there is limited ability to vary the order in response to any actions that the cloud providers may take to introduce these technical frictions elsewhere in their ecosystems.[41]

[40] CC3 (Revised), Guidelines for market investigations: Their role, procedures, assessment and remedies Annex B, Paragraph 53: The [CMA] will have particular regard to avoiding circumvention risk in implementing measures limiting the behaviour of firms with significant market power that has been found to prevent, distort or restrict competition. This is because firms with significant market power may readily evolve new forms of behaviour to replace prohibited or restricted conduct.

[41] We note that the CMA has the ability to vary market investigation orders under section 162 of the Act, and that this provides some flexibility to address issues that may be affecting the effectiveness of such orders. We further note that the DMCC Act amends the Act (see section 162A of the Act) to introduce additional powers to vary market investigation orders, which, depending on how and when the Government commences these new powers, may possibly apply to any market investigation order implementing remedies following the publication of our final report in this investigation. However, as set out above, we consider that in this case, a remedy that would serve as a comprehensive solution to the identified AEC may need to be able to be iterated and revised more periodically than is practicable through use of the remedy review provisions of sections 162 and 162A.

The standards setting body

W.51 We have not identified any existing entities that would be well suited to act as a standard setting body for relevant cloud services, to assist with the implementation of standardisation remedies through a market investigation order. While open-source foundations have some beneficial characteristics, we consider that they were not designed to oversee a CMA remedy and their existing structures, particularly their governance structures, are unlikely to be naturally well suited to this task, and so there are risks in seeking to rely on them as an integral part of a remedies package. Such concerns are exacerbated by a lack of sufficient flexibility in the market investigation order, such that it would be difficult to refine the requirements and design over time.

W.52 In the absence of an existing entity, a new independent oversight entity with sufficient relevant expertise to oversee the development, implementation and ongoing maintenance of the common standards would likely be required.

W.53 As noted above, we consider that seeking to establish a new entity for this purpose is challenging and has implications for the effectiveness of the approach, particularly from the extended timescales that would be required to set up the body, substantial complexity and the potential that the body is ineffective because of a lack of technical capability, resources/funding and/or other practical considerations.

W.54 We consider that the risk associated with identifying or establishing a standards setting body is common across IaaS, PaaS and ancillaries, and applies to both the features of the cloud services and their interfaces.

The cloud providers in scope

W.55 As discussed above, there are benefits in targeting the remedy at a small number of larger providers. In particular, since the cloud services market is concentrated larger firms have a greater incentive to maintain or increase technical barriers to switching and multi-cloud while smaller providers have a greater incentive to reduce barriers, including by voluntarily adopting standards.

W.56 Narrowing the number of cloud providers in scope of the remedy (eg to AWS and Microsoft) would also simplify some of the practical difficulties, such as monitoring compliance with the standard, and hence reduce the associated risks. However, smaller suppliers should not be excluded from the process, as this would raise concerns about the larger suppliers, such as AWS or Microsoft, having undue influence over the development and/or maintenance of these standards.

W.57 Therefore, we consider that smaller providers should be consulted as part of the process to develop standards, and it may be beneficial for smaller providers to

implement the standards themselves. However we do not consider it to be necessary to require their participation as their incentives would lead them to seek to increase interoperability, particularly with the larger suppliers.

W.58 Accordingly, we consider that a standardisation remedy could be effective if at least AWS and Microsoft were in scope of its requirements.

Monitoring compliance and enforcement

W.59 We considered there to be monitoring and enforcement risks, in ensuring that the independent body appointed to develop and provide oversight of the technical standard had the ability to monitor compliance and to effectively enforce against non-compliance. There would need to be clear delineation of roles and responsibilities between any bodies involved in oversight more broadly and a mechanism for setting and enforcing sanctions.

W.60 We considered that this risk would be particularly acute for any standards being applied to cloud services where there was greater scope for ongoing change (eg PaaS), as these circumstances would necessitate closer and more detailed ongoing assessment.

Timescales

W.61 We considered the timescale over which standardisation remedies would be likely to take effect and the impact on customer detriment.

W.62 Where the CMA is taking action itself, the implementation of the remedies following a market investigation typically involves the CMA making an order or accepting undertakings, which it must do within six months of the date of publication of the final report.[42]

W.63 However, we would expect there to be a substantial implementation period following the issuance of the relevant legal instruments. Establishing an independent oversight body, with subsequent technical work to develop the relevant standards would likely be a lengthy endeavour.

W.64 The exact time to design and implement any individual standards would vary depending on the specific circumstances (eg depending on the technical complexity).

[42] The Act, Section 138A. The CMA may extend the six-month period only once and by up to a further four months if it considers that there are special reasons why a final order cannot be made within the statutory deadline.

Interactions with other laws and regulations

W.65 We recognise that regulatory authorities in other jurisdictions could introduce and require cloud providers to follow particular standards. For example, we are aware that the EU Data Act includes clauses which allow the EU to introduce standards that require cloud providers to ensure compatibility with common specifications based on open interoperability specifications or harmonised standards for interoperability within 12 months of a standard being introduced.[43]

W.66 While the broad aims of open interoperability specifications and harmonised standards under the EU Data Act are likely to align with the aims of any standards that we might introduce to improve interoperability and reduce technical barriers to switching and/or multi-cloud, there is the potential for inconsistencies and contradictions in how standards are designed and implemented.

W.67 This potential for regulatory fragmentation also extends to other standards introduced in other jurisdictions. To mitigate this risk, effective monitoring of any new standards would be essential as would the ability to iterate any remedies to address any inconsistencies and/or contradictions that might arise.

Our assessment

W.68 We consider that standardisation remedies in cloud would typically be complex, technical and likely to need continuous oversight and refinement both in terms of the scope of the remedy (eg which services are included) and the specific standards (eg maintaining the design of the technical standard itself).

W.69 At this stage, we consider that it would be difficult to identify a specific set of services for which common standards should be implemented through a market investigation order and that would effectively address the AEC we have provisionally found. We consider that identifying the services to which common standards should be implemented needs to weigh up the likely benefits of standardisation with the risk of distorting the cloud services market, for example, by reducing the potential for innovation. We recognise that such an assessment may need to reflect that the harm attributable to individual services is likely to vary over time because of technological changes, new design choices and/or the scope for future innovation.

W.70 We note that the need for a careful assessment of the benefits of a standard against its risks is especially acute in relation to more differentiated PaaS services. However, we also consider that even for services less prone to distortion risks, such as ancillary services, IaaS and APIs, there would still be a need for flexibility and iteration in the implementation of any standardisation remedy in order to

[43] EU Data Act: Article 30: 3. Regulation - EU - 2023/2854 - EN - EUR-Lex, last accessed 24 October 2024.

address residual distortion risks, swiftly address technological or service-design changes that the standards might need to adapt to, and to test and trial the standards so that they could be efficiently refined or recalibrated.

W.71 There is also a concern that in response to the imposition of standards for certain cloud services, cloud providers, and particularly the largest cloud providers, would reintroduce technical frictions elsewhere in their ecosystems, essentially circumventing the intent of the standard. To mitigate this concern, we consider that it would be necessary to include an independent oversight mechanism, most likely through the establishment of an oversight body. However, we recognise that doing so introduces its own risks, in particular around the design of that body and the timelines required to establish it.

W.72 The oversight mechanism would also need to be part of a wider monitoring and compliance system. This is likely to need to be relatively detailed, to reflect the technical complexity and the presence of information asymmetries between the companies and any oversight body,[44] as well as needing to adapt and respond to any changes, such as technical advancements, which have implications for the existing or potential new standards.

W.73 We consider that the risks related to monitoring and implementation, including in relation to the establishment of an oversight body, could in principle be addressed through a market investigation order in many cases. However, in light of our recommendations to the CMA Board to prioritise commencing SMS investigations into AWS' and Microsoft's digital activities in respect of cloud services, this could, were the CMA to designate one or both of these firms with SMS in cloud services, introduce what amounts to an overlapping regulatory regime.

W.74 Therefore while, in principle, a market investigation order that requires increased standardisation of some cloud services and/or interfaces could address the harm arising from some of the individual technical frictions, considering the combination of risks we have identified above, our provisional view is that a market investigation order is unlikely to give sufficient flexibility to design, implement, monitor and enforce standardisation remedies in a way that would make it part of a comprehensive solution to the AEC we have provisionally found.

Requiring cloud providers to offer abstraction layers (Potential remedy 5)

W.75 Abstraction layers abstract the functionality between cloud providers, improving customers' ability to manage their multi-cloud architecture and switch between providers.

[44] CC3 (Revised), paragraph 378.

W.76 These services and similar services that also promote interoperability, such as platforms that provide infrastructure as code and inter-cloud brokers, rely on accessible, open APIs. We consider the availability of accessible, open APIs to be fundamental to a functioning cloud market.

W.77 In this section we consider the design considerations for a remedy to require cloud providers to offer abstraction layers, before commenting on the effectiveness of the remedy.

Design considerations

W.78 We have considered the following elements in the design of this remedy:

(a) which cloud services are in scope;

(b) what is the technical specification; and

(c) which cloud providers are in scope.

Cloud services in scope

W.79 We considered that any requirement for cloud providers to offer abstraction layers should currently be limited to abstracting IaaS services.

W.80 There is less differentiation between cloud providers in IaaS services compared to PaaS services. Requiring cloud providers to offer abstraction layers would act to commoditise IaaS, giving customers more ability to use IaaS and PaaS from different cloud providers, reducing the incentive/necessity for customers to use IaaS services from the same provider that they use for PaaS services.

W.81 We considered that any customer benefits that arise from differentiation in IaaS services may be relatively modest compared to PaaS services, given the greater commonality that currently exists in the IaaS services that are offered by the different cloud providers.

W.82 We also considered that the cloud providers would still be incentivised to invest in operating efficiencies in IaaS, as increased commonality and increased ability to switch through the use of abstraction layers, would incentivise them to compete more vigorously, most likely by offering lower prices.

Technical specification

W.83 Any abstraction layer that cloud providers offered would need a technical specification for the abstraction layer. The specification could include detailed technical requirements, alongside general principles that the providers would need to comply with.

Cloud providers in scope

W.84 Due to the costs involved in developing abstraction layers or similar solutions, we considered that any remedy should be limited to a small number of large providers.

W.85 Requiring large cloud providers, such as AWS and Microsoft, to offer abstraction layers also has the potential to create distortions in the cloud services market if the companies in scope sought to use this requirement to their own benefit. For example, the companies could:

(a) design the abstraction layers so that they integrate better with their own, first party cloud services.

(b) lock customers into the abstraction layers, reducing their ability to switch.

(c) implement abstraction layers that function in a unidirectional manner (eg by allowing customers to use the abstraction layers to combine third party IaaS with these providers' own PaaS, but creating barriers to the use of third party PaaS with their own IaaS).

W.86 AWS and Microsoft have a combined share of the IaaS and PaaS markets of 60-70% (and a combined 80-90% share of the IaaS market). The introduction of abstraction layers by AWS and Microsoft would increase the potential for customers to use cloud services from a smaller provider in conjunction with the cloud services of AWS and/or Microsoft. Therefore, if at least AWS and Microsoft were in scope, this would encompass a large majority of UK customers, and accordingly we have focused our assessment on AWS and Microsoft.

Effectiveness assessment

W.87 Abstraction layers offered by large cloud providers, such as AWS and Microsoft, could allow their customers to use IaaS from other cloud providers and/or use their primary provider's IaaS with PaaS hosted on other clouds. This would increase the ability of customers to use multiple clouds and to switch between clouds, which in turn could increase competition between cloud providers, with cloud providers having more incentive to compete due to lower barriers to switching.

W.88 However, as noted above, we considered that requiring large cloud providers to offer abstraction layers would present risks of distortion. These large providers could lock customers into the abstraction layer(s), better integrate their own first party services with the abstraction layer(s) and/or use the abstraction layer(s) to expand their own ecosystem(s).

W.89 We also consider that there is a risk associated with developing a technical specification for an abstraction layer.

W.90 In summary, we see the benefits in abstraction layers that are offered by third parties in assisting customers using and switching between IaaS and PaaS across multiple clouds. We also recognise the role that cloud providers need to play in maintaining open APIs to allow third parties to offer abstraction layers and similar services such as platforms that offer infrastructure as code.

W.91 However, we do not consider that requiring large cloud providers (such as AWS and Microsoft) to offer abstraction layers would be an effective remedy, due to the risks of distortion and the risk associated with setting the technical specification.

Increasing interconnectivity and/or reduce latency (Potential remedy 6)

W.92 In our working paper on technical barriers, we included two potential remedies to increase interconnectivity and reduce latency, which involved:

(a) connecting third party data centres; and

(b) requiring cloud providers to make data centre space available for other cloud providers.[45]

W.93 In the working paper we recognised that these potential remedies have particular risks, including potential implications for cloud providers' incentives to invest in data centres and cloud infrastructure more generally. We concluded that we were not minded to prioritise either potential remedy for further investigation.[46]

W.94 We have not received any submissions in response to our working paper that causes us to change this view.

Increasing transparency around the interoperability of cloud services (Potential remedy 7)

W.95 Below we consider the design considerations and the effectiveness of a potential intervention to require cloud providers to give customers sufficient detailed information on the lock-in risks associated with their cloud services.

Design considerations

W.96 We have considered the following elements in the design of this remedy:

(a) what information should the cloud providers publish;

(b) how accessible is the information;

[45] Technical barriers working paper, paragraphs 9.90-9.112.
[46] Technical barriers working paper, paragraph 9.92.

(c) which cloud providers are in scope;

(d) which cloud services are in scope; and

(e) how is the remedy monitored and enforced.

Information required

W.97 Cloud providers currently publish some information on the lock-in risks associated with their cloud services and they also publish information that shows how to migrate from one cloud service to another. However, the quality and depth of information varies between cloud services and between cloud providers.

W.98 We also note that while cloud providers have an incentive to assist customers in migrating to their cloud services, they are not incentivised to assist customers in migrating away from their cloud services.

W.99 We considered whether a remedy should require cloud providers to disclose additional details on lock-in risks and migration journeys to customers, which would include information such as:

(a) An explanation of whether the software provided by the cloud service is open-source or proprietary.

(b) An explanation on the extent to which the service requires integration with non-open source, proprietary features offered by the cloud provider to function effectively.

(c) An explanation on the extent to which similar cloud services are offered by other cloud providers and the extent to which the cloud provider's own cloud service is different from those of its competitors.

(d) Information on the lock-in risk associated with each cloud service. We are aware of at least one more sophisticated customer who monitors differentiation of services between cloud providers and assigns a grade to the lock-in risk associated with each cloud service. It would be beneficial for cloud providers to make such information available to all customers.

(e) Standard actions that a customer would need to take to migrate away from the cloud service to an equivalent service on another cloud (assuming an equivalent service exists). This could take the form of a guide showing how to migrate away from the cloud service.

W.100 There are practical considerations associated with defining the amount of detail that the cloud providers would be required to disclose. Too much detail and customers may struggle to engage with the material. Too little detail and the

information that is disclosed would not be sufficient for customers to make informed decisions.

W.101 We also considered that if the requirements were not sufficiently well defined, cloud providers may attempt to circumvent the intent of the remedy by disclosing insufficient and/or irrelevant information. For this reason, we considered that there would be benefit in being able to iterate the information requirements to address this circumvention risk, particularly if technologies change over time.

W.102 We also noted that both the Data Act[47] and the French SREN legislation of cloud services[48] also include transparency obligations, and Arcep the relevant French authority are currently consulting on what such a 'technical reference offer' should include.[49] This includes similar considerations as those we have set out above.

Accessibility

W.103 The information specified above would need to be accessible to customers, which would be the case if it was included or linked in the product specification for each cloud service. By product specification we mean the technical documentation that explains to customers what a cloud service does and how it functions. Product specifications could be included or linked on the webpage that customers use to access the service.

Cloud providers in scope

W.104 We consider that there is benefit in targeting the remedy at a small number of larger providers. This is because:

(a) the cloud services market is concentrated, for example AWS and Microsoft have a combined share of the IaaS and PaaS markets of 60-70%. Therefore, the majority of customers in the cloud services market would benefit directly from the remedy covering a small number of suppliers.

(b) the largest firms have the greatest incentive to adopt defensive strategies to ensure that they retain their large existing customer bases. This means that there is likely to be proportionately more benefit in requiring AWS and

[47] EU Data Act: Articles 25 and 26. Regulation - EU - 2023/2854 - EN - EUR-Lex, last accessed 24 October 2024. Article 26(b) says that the provider must 'provide the customer with… a reference to an up-to-date online register hosted by the provider of data processing services, with details of all the data structures and data formats as well as the relevant standards and open interoperability specifications, in which the exportable data referred to in Article 25(2), point (e), are available.' Article 25(2)(e) is a provision stating that the contract must include an 'exhaustive specification of all categories of data and digital assets that can be ported during the switching process, including, at a minimum, all exportable data'.
[48] SREN: Security and Regulation of the Digital Space: Article 29 II, last accessed 18 November 2024.
[49] ARCEP: Public consultation on the regulation of cloud services, last accessed 18 November 2024.

Microsoft to better explain lock-in risks to customers and how to migrate away from their cloud services than there would with smaller cloud providers.

(c) we also consider that smaller cloud providers have more incentive for their cloud services to be interoperable, which lessens the risk of lock-in compared to AWS and Microsoft.

W.105 There are also practical benefits of having fewer firms in scope of these remedies, as it would reduce complexity and associated levels of resource required for implementation, monitoring and enforcement.

W.106 We note that by restricting the remedy to AWS and Microsoft, there is a risk of distortion. However, for the reasons noted above, we consider the risk of distortion to be low.

Cloud services in scope

W.107 We considered that this remedy could apply to all cloud infrastructure services, including IaaS, PaaS and ancillaries. The reason for including these cloud services in scope is that lock-in risk and how to migrate away from a cloud service are relevant considerations for customers when choosing any cloud service.

Monitoring and enforcement

W.108 In general, we considered the monitoring and enforcement risk associated with this specific remedy to be relatively low. However, we considered that:

(a) monitoring would require technical input to assess whether the cloud providers were compliant.

(b) any instances of non-compliance and subsequent enforcement action may rely, at least in part, on subjective judgement. This risk could be mitigated by allowing the specification of the remedy to be iterated to reduce the potential for dispute.

Effectiveness assessment

W.109 We set out our effectiveness assessment under the following headings:

(a) implementation;

(b) monitoring and enforcement; and

(c) timescales.

Implementation

W.110 The benefits of this remedy include:

(a) improving customer awareness of potential lock-in risks prior to customers using a cloud service.

(b) allowing customers to better identify more interoperable and portable solutions and providing customers with clearer guidance on how to use them.

(c) informing customers of the steps they would need to take to migrate away from a cloud service and allowing customers to develop better exit strategies.

W.111 We noted that clear, useful, visible information on the risk of lock-in is most likely to assist new, smaller customers who may have less existing understanding of these risks.

W.112 In addition to the benefits, we have also identified certain risks associated with the effectiveness of the remedy. The risks include:

(a) the specification of the information that cloud providers would be required to publish being insufficiently clear or useful.

(b) information on lock-in risks associated with a cloud service not being accessible to customers prior to committing to a cloud service.

W.113 We also noted that if the technical specification was not adequately defined, it would increase the scope for circumvention of the remedy.

W.114 We considered that these risks could be mitigated by precise remedy design and requiring cloud providers to adhere to a mix of rules and guiding principles.

Monitoring and enforcement

W.115 We considered the risks associated with monitoring and enforcement to be relatively low, given that the scope of the remedy would be on only two cloud providers and the information that we would require cloud providers to disclose for each cloud service would be limited.

Timescales

W.116 We considered that an information transparency remedy to improve customer awareness of lock-in risks and the steps required to migrate away from a cloud service could be implemented reasonably quickly by the cloud providers.

Our assessment

W.117 Our provisional view is that an information transparency remedy could improve customer awareness on the lock-in risks and portability of cloud services and inform them how to migrate away from cloud services. We consider that a transparency remedy could be implemented through a market investigation order but we are of the provisional view that this would not on its own be an effective remedy to the technical barriers that we have provisionally found to be contributing to an AEC, as information transparency remedies:

(a) do not reduce the prevalence or impact of technical barriers that are currently present in cloud services.

(b) will benefit some customers, particularly those who have yet to migrate some or all their workloads to the cloud, but they are likely to have a more limited benefit to:

(i) customers who have already migrated most of their workloads on to the cloud, as they have already made decisions on how their systems are architected, the extent to which they are locked in and how difficult it would be for them to migrate away from a cloud service.

(ii) the most sophisticated customers who are likely to have some pre-existing awareness of lock-in risks and/or better understanding of how to migrate away from cloud services.

Requiring cloud providers to make training and education courses cloud agnostic (Potential remedy 8)

W.118 A lack of skills can restrict customers' ability to use multiple clouds and switch between clouds.

W.119 A remedy to require cloud providers to make training cloud agnostic could, in principle, improve the ability of cloud engineers to work across multiple clouds.

W.120 However, in practice, requiring training courses to include some cloud agnostic training appears unlikely to be sufficient to bridge any gap in skills that would allow engineers to work on multiple clouds. Instead, it has the potential to make training less useful to participants' needs.

W.121 This could act to deter UK-based cloud engineers from undertaking some training, which could have a detrimental impact on their overall skill level.

W.122 We also noted that there are several specification risks associated with the implementation of a requirement for more cloud agnostic training, which would

result in any skills based remedy being difficult to monitor and enforce. These include:

(a) what constitutes cloud agnosticism; and

(b) what training falls in scope, for example, should the remedy be restricted to formal, instructor-led training courses?

W.123 Our provisional view is that requiring cloud providers to offer cloud agnostic training would not be an effective remedy.

Our views on remedies to technical barriers that could be implemented through a market investigation order

W.124 We have set out our assessment and provisional views on each of the potential remedies to technical barriers that we have identified during the course of this investigation. In particular:

(a) we have examined the case for standardisation of IaaS, PaaS, ancillary services and APIs. We consider that in designing any standardisation remedies there would be a need for a careful assessment of the benefits of a standard against its risks, in order to correctly identify—especially in light of the danger of distortion risks—the services for which the risks would be outweighed by the benefits.

(b) for more differentiated services, such as some PaaS services, the distortion risks of standardisation could be particularly high. We consider that even for ancillary services and IaaS and also for APIs, where in principle there is greater scope for standardisation, there is still benefit from flexibility and iteration in the implementation of the remedy. This would be important in addressing residual distortion risks and technological or service design changes that the standards might need to adapt to. It would also benefit from testing and trailing of standards so that they could be refined or recalibrated efficiently.

(c) accordingly, a key element in the design of a standardisation remedy would be the ability to iterate the remedy in response to technical changes, new innovations or the re-introduction of technical frictions in an attempt to circumvent the aim of the remedy. This would require a level of flexibility to the design, implementation, monitoring and enforcement of remedies that would be challenging to achieve through a market investigation order.

(d) we consider that a transparency remedy could be implemented through a market investigation order but we are of the provisional view that this would not be an effective remedy on its own, as information transparency remedies would not reduce the prevalence or impact of technical barriers that are

currently present. Furthermore, there is limited benefit to customers who have already migrated to the cloud or to more sophisticated customers, who have some pre-existing awareness of lock-in risks.

(e) we are of the view that requiring the largest cloud providers to offer abstraction layers, potential remedies to reduce latency and a remedy to require more cloud agnostic training (potential remedies 5, 6 and 8) are currently likely to face greater challenges to their effectiveness, including risks that are unlikely to be addressed by expanded remedial powers such as the ability to iterate or to test and trial remedies in advance of implementation.

W.125 In light of these assessments, our provisional view is that, although in principle a package of remedies implemented through a market investigation order could address these technical barriers, there are likely to be material risks associated with these remedies such that it would be very difficult to achieve a comprehensive solution through the use of the remedy-making powers under the Act.

W.126 We consider that if the CMA were to designate AWS and Microsoft with SMS in respect of cloud services and consider the imposition of appropriate interventions such as those considered in this report, it would have the ability to test and trial remedies, as well as to iterate remedies over time, which we consider would likely address many (if not all) of the major risks we have identified in our assessment.

Egress fees

Description of the potential remedy

W.127 The potential remedy would control the level of egress fees for all switching and multi-cloud egress data transfers via the internet in the UK. This would limit the charges that UK customers pay to transfer their data from one cloud to another cloud for the purposes of switching or using multiple public cloud services.

W.128 This remedy could also include a requirement for cloud providers to clearly display the egress fees applicable to cross-cloud egress on public and personalised data transfer pricing pages and show the pricing in a prominent and specific (ie unbundled) way in any price estimates where egress services are included.

Stakeholder views

W.129 Submissions from stakeholders, largely in response to our egress fees working paper, are summarised below.

Submissions received on the need for, and suitability of, egress fees remedies

W.130 AWS, Microsoft and Google all submitted that remedies for egress fees were unnecessary and/or would not address any perceived concern about customer switching and multi-cloud use.[50]

W.131 AWS and Google submitted that their elimination of egress fees globally (including in the UK) for switching customers removes any potential concern around egress fees for switching.[51]

W.132 Microsoft submitted that egress fees do not currently drive customer behaviour, and if the CMA were to intervene by forcing egress fees to a level below cloud providers' costs (and a return on investment) or to prohibit them completely, this would be unlikely to have a meaningful impact on switching or multi-cloud solutions. However, Microsoft submitted that this form of intervention would likely lead to excessive and inefficient usage of the cloud.[52]

W.133 Microsoft also said that, although it does not believe egress fees impact switching or multi-cloud, any remedies should be aligned with EU rules to avoid confusion for its customers.[53]

W.134 IBM submitted that an information transparency remedy would be sufficient to address any perceived issues with egress fees, without the need for stronger price control remedies, and was of the view that a complete ban of egress fees was unwarranted and not efficient as it submitted that egress fees are not the main nor one of the main barriers to switching and multi-clouding.[54]

W.135 Some cloud providers support data egress being free for customers.[55] They provided the following rationales for this view:

(a) Oracle said data mobility fees should be zero. Oracle said that cloud providers should not be competing on data transfer fees as it considers that the value it provides to customers is based on its service offerings. It also noted that as data remains the property of the customers, the customer

[50] AWS' response to the CMA's updated issues statement and working papers, paragraph 29; Microsoft's response to the Competitive Landscape, Committed Spend Agreements and Egress Fees Working Papers, paragraphs 92-93; Google's response to Egress fees working paper, paragraph 57.
[51] AWS' response to the Egress fees working paper, paragraph 32; Google's response to the Egress fees working paper, Annex response (b).
[52] Microsoft's response to the Competitive Landscape, Committed Spend Agreements and Egress Fees Working Papers, paragraph 83.
[53] Summary of hearing with Microsoft, paragraph 67.
[54] IBM's response to Egress fees working paper, pages 1-2.
[55] OVHcloud response to issue statement, dated 17 October 2023, page 15; Oracle response to the Issues Statement, dated 17 October 2023, page 5.

should be readily able to move their data among various cloud services and providers.[56]

(b) OVHcloud said it considers egress fees to represent artificial costs and to be unduly used by the largest cloud providers to lock customers in their ecosystems and prevent them from switching.[57]

(c) Wasabi, a smaller cloud provider, submitted that egress fees can create artificial barriers and unfairly penalize customers for their data mobility, and that this not only hampers competition but also stifles innovation by discouraging customers from using their data, and/or exploring alternative solutions.[58]

W.136 Customers submitted varying views on the suitability of egress fees remedies and their likely impact:

(a) A banking provider submitted that a reduction and (ideally) the removal of egress costs, rather than pitched to deter full or partial switching, would enhance flexibility and reduce the cost of data replication;[59]

(b) Vodafone submitted that the reduction of egress charges will be seen by enterprises as an enabler and supported a wider application of data egress policy to non-switching scenarios.[60]

(c) A telecommunications company submitted that disproportionate interventions or restrictions on egress fees, such as a full ban or caps could have unintended consequences, particularly where it is not clear that they address a consumer choice issue nor are targeted at a specific competition issue.[61]

(d) Another customer submitted that reducing or eliminating egress fees will not impact switching or duplicative multi-cloud because egress fees are a small consideration compared to the required staff investment, but that remedies to address barriers to operating integrated multi-cloud would have a demonstrably positive impact on competition and that this is where interventions should be focussed.[62]

---

[56] Oracle response to the Issues Statement dated 17 October 2023, page 5.
[57] OVHcloud's submission to the CMA [✂].
[58] Wasabi's response to the Working papers dated 23 May 2024 and 06 June 2024, pages 1 to 2.
[59] Banking Provider 1's response to the Updated issues statement and Working papers dated 23 May 2024 and 06 June 2024, page 1.
[60] Vodafone's response to the Working papers dated 23 May 2024 and 06 June 2024, pages 1-2.
[61] [✂] submission to the CMA [✂].
[62] [✂] submission to the CMA [✂].

Submissions received on remedy design

W.137 We received limited submissions on remedy design in response to the egress fees working paper. The submissions received on duration, market-wide application, and product scope are set out below.

W.138 Google submitted that any price control remedies for egress fees should only apply to cloud providers with significant market power.[63] Google submitted that any restrictions on egress fees should continue to apply for as long as a cloud provider retains market power (with appropriate sunset and/or review clauses).[64]

W.139 Google and another cloud provider submitted that a market-wide ban on egress fees would have a more detrimental and disproportionate impact on smaller cloud providers such as themselves that would not be able to recover costs and/or investment through their customer base.[65]

W.140 [✂].[66]

W.141 AWS, Google and IBM submitted that direct connections should not be in scope of any potential remedies and Microsoft submitted that any potential remedies should be limited to internet egress routed via the ISP network.[67] Microsoft submitted that limiting the remedy to ISP routing egress retains flexibility for cloud providers to provide premium egress services and allows cloud providers to charge fees that recoup their costs and a reasonable return on their investments.[68] Microsoft submitted that limiting scope to internet egress via ISP would impact the most price-sensitive customers as well as retaining incentives for cloud providers to invest in and to build out low-latency and premium offers.[69]

W.142 One cloud provider submitted that a one-size-fits-all remedy, applying in particular both to customers switching or multi-clouding, is unlikely to be the best solution for the market.[70]

W.143 AWS, Google and IBM raised issues with the ability to identify the purpose of transfers and the use of identification data associated with data transfers (eg Border Gateway Protocol (BGP) peer Autonomous System Number (ASN)) as a

---

[63] Google's response to the Egress fees working paper, Annex response (a).
[64] Google's response to the Egress fees working paper, Annex response (a).
[65] Google's response to the Egress fees working paper, paragraphs 3c) and 58-59; [✂] submission to the CMA [✂].
[66] [✂] submission to the CMA [✂].
[67] AWS' response to the Egress fees working paper, heading D and paragraph 29; Google's response to the Egress fees working paper, Annex response (a); IBM's response to Egress fees working paper, page 2; Microsoft's response to the Competitive landscape, Committed spend agreements and Egress fees working papers, paragraph 9.
[68] Microsoft's response to the Competitive landscape, Committed spend agreements and Egress fees working papers, paragraph 9.
[69] Microsoft's response to the Competitive landscape, Committed spend agreements and Egress fees working papers, paragraph 100.
[70] [✂] submission to the CMA [✂].

proxy for identifying switching and multi-cloud egress.[71] AWS and IBM considered there to be issues such as ASNs not being accurate in identifying networks for use of cloud services specifically.[72] Google and another cloud provider submitted that customers may not be happy with cloud providers accessing data associated with data transfers to determine transfer destination.[73]

Submissions received on approaches to determining the level of fees

W.144 We received some submissions from cloud providers and a customer which made specific points on a potential remedy capping egress fees based on costs incurred:

(a) AWS submitted that price controls are costly to implement and may not even be workable due to the complexity of costs associated with data transfers. AWS also submitted that capping egress fees at cost may force providers to increase prices of other cloud services in order to maintain positive margins.[74]

(b) Google submitted that setting a fee cap using fixed list of cost items would likely result in significant practical challenges around implementation and compliance, and disproportionately affect a challenger like Google who has invested heavily in providing a broader range of high-quality networking products and services. It also said it could result in less pricing transparency for customers if certain networking cost items that are not on the permitted list end up being embedded in, and recovered through, the pricing of non-networking cloud products and services, and more price uncertainty if fees fluctuate based on the underlying cost items.[75]

(c) IBM submitted that price control remedies are not warranted in relation to egress fees and would be challenging to implement in practice as identified by the CMA's egress fees working paper. IBM said that if price controls are considered necessary, then this should be framed by reference to costs, and not other fees charged by the cloud provider.[76] In relation to IBM's compliance with the EU Data Act's current provisions for providing switching egress at cost, IBM submitted that [✂].[77]

(d) Microsoft submitted that the concerns it raised about the clarity and predictability of cloud spend for customers, if egress fees were set to a level below cloud providers' costs (and a return on investment) or banned, would

[71] AWS' response to the Egress fees working paper, paragraphs 21-23; Google's response to the Egress fees working paper, Annex response (e); IBM's response to the Egress fees working paper, pages 2-3.
[72] AWS' response to the Egress fees working paper, paragraph 22; IBM's response to the Egress fees working paper, pages 2-3.
[73] Google's response to the Egress fees working paper, Annex response (e); [✂] submission to the CMA [✂].
[74] AWS' response to the Egress fees working paper, paragraphs 26 and 28.
[75] Google's response to Egress fees working paper, Annex response (f).
[76] IBM's response to Egress fees working paper, page 2.
[77] [✂] submission to the CMA [✂].

particularly apply if complex mechanisms were created to determine accepted charges.[78]

(e) One customer submitted that there is nothing to indicate AWS would feel constrained to recover only its costs under a price cap, and that given the opacity of cloud costs (and the lock in effects which the customer said it feels acutely), it is highly unlikely that customers would be able to tell whether cloud providers were doing so or whether they were seeking to recover all their lost revenue and more.[79]

W.145 Many of the same potential risks and disadvantages of an egress fees ban raised by AWS, Microsoft and Google (which we set out in further detail below, eg potential price rises for other services, risk of inefficient egress and disincentive to invest and innovate) were also submitted as applying to a price cap at cost.[80]

W.146 We received very limited submissions on a potential remedy capping egress fees by reference to other fees charged specifically, and of those we did receive, none were in favour of this approach over other proposed options.

Submissions received on potential risks of an egress fees cap or ban

W.147 A number of potential risks for a remedy that caps the level of egress fees were identified by cloud providers (primarily AWS, Microsoft and Google).

W.148 AWS, Microsoft and Google submitted that remedies to regulate egress fee prices would risk reduced investment in network infrastructure and quality and/or innovation.[81]

W.149 AWS, Microsoft, Google and IBM submitted that a remedy to ban or lower egress fees could lead to cloud providers recovering costs (or for Microsoft, recovering costs and return on investment) through other means, such as price increases for other services.[82] AWS, Microsoft and Google submitted that this may be unfair to some customers as customers with small or no egress usage may then subsidise

[78] Microsoft's response to the Competitive landscape, Committed spend agreements and Egress fees working papers dated 23 May 2024, paragraph 83.
[79] [✂] submission to the CMA [✂].
[80] AWS' response to the Egress fees working paper, paragraph 28; Microsoft response to the competitive landscape, committed spend agreements and egress fees working papers, paragraph 83; Google's response to Egress fees working paper, paragraph 21.
[81] AWS' response to the Updated issues statement and working papers, paragraph 32; Microsoft's response to the Competitive landscape, Committed spend agreements and Egress fees working papers, paragraphs 9 and 83; Google's response to Egress fees working paper, paragraph 57 and Annex response (h). Note, cloud providers' submissions on investment and innovation are also set out in Chapter 5, Egress fees.
[82] AWS response to the Issues Statement dated 17 October 2023, paragraph 29; AWS' response to the Egress fees working paper, paragraphs 15 and 28; Microsoft's response to the Competitive landscape, Committed spend agreements and Egress fees working papers, paragraphs 97-99; Summary of hearing with Microsoft, paragraph 66; Google response to the Issues Statement dated 17 October 2023, paragraph 30(a); IBM's response to the Egress fees working paper, page 2.

larger egress users.[83] Oracle agreed that if the costs incurred by a cloud provider are not recovered in one form, they will likely be recovered elsewhere, in order to allow the provider to achieve an economic return.[84]

W.150 AWS, Microsoft, Google and another cloud provider also submitted that a ban on egress fees risks inefficient egress usage by customers, potentially resulting in overuse of network infrastructure or capacity.[85] Microsoft submitted that an egress fee ban would lead to data resilience security risks arising from the already significantly high and increasing volume of data traffic via cloud infrastructure.[86]

W.151 IBM submitted that customers' need for an efficient IT infrastructure is only relevant to multi-cloud use, as this is less relevant when switching cloud provider entirely.[87]

W.152 A [✂] cloud provider was not in favour of banning egress fees, but on the basis that smaller providers and new entrants to the cost-intensive IaaS market do not have the requisite capital or scale to cross-subsidise and offer egress for free as it suggested the large cloud providers do. It said that an egress ban risks entrenching hyperscalers' oligopoly leading to less competition.[88]

W.153 Microsoft also submitted that banning or setting egress fees artificially low through regulation would distort prices such that they are not reflective of the true underlying costs and value provided and would break the existing cloud model of customers paying for actual services consumed.[89] Microsoft submitted that clarity and predictability of cloud spend for customers will be undermined without the connection between customers' consumption of data transfer services and their payment for that service.[90]

W.154 Two academics submitted that price regulations for egress fees would not be beneficial.[91] One submitted that the potential remedies set out in the CMA's

---

[83] AWS' response to the Issues Statement dated 17 October 2023, paragraph 29; Summary of hearing with Microsoft, paragraph 66; Google's response to the Issues Statement dated 17 October 2023, paragraph 30(b).
[84] Oracle's response to the Updated issues statement and working papers, page 3.
[85] AWS' response to the Egress fees working paper, paragraph 17; Microsoft's response to the Competitive landscape, Committed spend agreements and Egress fees working papers, paragraphs 9 and 95; Google's response to the Egress fees working paper, paragraph 57 and Annex response (h); [✂] submission to the CMA [✂]. Note, cloud providers' submissions on the risk of inefficient egress usage are also set out in Chapter 5, Egress fees.
[86] Microsoft's response to the Competitive landscape, Committed spend agreements and Egress fees working papers, paragraph 95.
[87] IBM's response to the Egress fees working paper, page 3.
[88] [✂] submission to the CMA [✂].
[89] Microsoft's response to the Competitive landscape, Committed spend agreements and Egress fees working papers, paragraph 95.
[90] Microsoft's response to the Competitive landscape, Committed spend agreements and Egress fees working papers, paragraph 83.
[91] R. Parisi, The Cloud Services Markets' Competitive Landscape: A contribution to the Competition and Markets Authority, page 14; Dr George R Barker. Comment on The UK Competitive Market Authority's (CMAs) Cloud Services Market Investigation Three Working Papers on The Supply of Public Cloud Infrastructure Services in the UK Covering the CMAs 1. Competitive Landscape Working Paper; 2. Egress Fees Working Paper; and 3. Committed Spend Agreements Working Pape, page 71. We note that Dr George Barker is a member of the Oxford Cross Disciplinary

egress fees working paper would have increasing adverse effects on competition in the market and as a result increasing detriment to consumers.[92]

W.155 We consider the risks raised in these submissions in our analysis below.

Analysis of the potential remedy for egress fees

Description of remedy and intended effect

W.156 We have provisionally found that the presence and relevance of egress fees to customers' decisions on switching and multi-cloud means that there is a weakened customer response to differences in price, service quality and/or innovation between cloud providers. As a result, egress fees contribute to a degree of 'lock-in' where customers are less able to switch cloud provider, or use multiple cloud providers, once they have made their initial choice upon entering the market(s) for cloud services.

W.157 Limiting or banning egress fees would seek to remove this feature as a commercial barrier to switching and multi-cloud. Supplemental pricing information transparency requirements would seek to address customer awareness about egress fees, making such information available and clearly presented. This would help customers to better exercise effective choice and respond to attractive offers for services from other cloud providers, without facing a cost constraint in the form of egress fees.

Design considerations

W.158 Below we discuss the key design, implementation and governance considerations for an egress fees remedy:

(a) The level of fees allowed;

(b) Cloud providers in scope;

(c) Egress services in scope; and

(d) Information transparency requirements.

Machine Learning Research Cluster (OXML), which is supported by Microsoft (see Dr George R Barker, Comment on The UK Competitive Market Authority's (CMAs) Cloud Services Market Investigation Updated Issues Paper and Working Papers 4-6 on The Supply of Public Cloud Infrastructure Services In the UK Covering The CMA's 1. Updated issues statement on Public cloud infrastructure services market investigation; 2. Licensing Practises Working Paper; 3. Technical Barriers; and 4. Potential Remedies page 1.

[92] Dr George R Barker, Comment on The UK Competitive Markets Authority's (CMAs) Cloud Services Market Investigation Three Working Papers on The Supply of Public Cloud Infrastructure Services in The UK Covering The CMAs 1. Competitive Landscape Working Paper; 2. Egress Fees Working Paper; and 3. Committed Spend Agreements Working Paper, page 71.

Level of fees allowed

W.159 Our egress fees working paper set out three options for setting the level of fees allowed under an egress fees price control:[93]

(a) Banning;

(b) Capping by comparison to costs; and

(c) Capping by comparison to other fees.

Banning

W.160 Banning egress fees would be analytically straightforward in terms of determining a methodology for setting the price of the fees in scope, given a ban sets the price to zero. Accordingly, a ban would result in a minimal specification or circumvention risk, as well as subsequent implementation, monitoring, and compliance risks.

W.161 We have not seen evidence to indicate that these risks differ between switching or multi-cloud egress data transfers, and so a ban could apply to both.

Capping by comparison to costs

W.162 We consider there to be substantially more specification risk for a price cap based on costs compared to a ban. There would be significant complexity associated with either a designated regulator or cloud providers determining the appropriate price cap methodology, with trade-offs between a 'lighter touch' guidelines approach which then has a greater monitoring and enforcement risk and regulatory burden (and potentially also circumvention risk), and a detailed price control determination to set an egress fee cap rate which required substantial time and resources and has higher design risk.

W.163 Cloud providers have indicated that there are a number of variable factors for determining the cost of a data transfer, such as geography (location and distance travelled), type of data transfer and changing supply costs over time.[94] This would create challenges for keeping any price cap set at an appropriate level over time, meaning that the design risk would be ongoing for the remedy's duration, and may even increase as a result of changes in the intervening time. It also means that there may be differences in costs for some cloud providers which could make a single price cap rate for all providers unsuitable, thereby creating either further

[93] Egress fees working paper, chapter 4.
[94] For example, Oracle submitted that cloud providers cannot determine with 100% accuracy how much cost will be incurred for each data transfer in real time, and that egress fee rates are a calculated assessment of how much it costs a cloud provider in terms of capital investment, intermediary charges (ie, to an ISP or other network provider), plus the amount of profit the cloud provider seeks to make on the transaction. Oracle's response to the Updated issues statement and working papers dated 23 May 2024 and 06 June 2024, page 1.

specification risk between providers, or further monitoring and enforcement risk due to the lack of comparable pricing.

W.164 Determining the relevant efficient costs to include in a price cap would be a challenge in general, given that cloud providers have some differences in their views of egress-specific costs and we found there to be substantial differences in the extent to which data transfer costs were tracked and/or allocated to egress specifically between cloud providers. We are also not aware of any cloud providers that track costs at the level of different types of egress, eg cross-cloud egress.

W.165 A price cap would also be less likely to achieve the intended aim of remedying egress fees as a commercial barrier for customers wishing to switch and multi-cloud, given that a cost to customers would remain which could continue to act as a commercial barrier.

Capping egress fees by reference to other fees charged by the cloud provider

W.166 Similar, and possibly greater risks, to those we have discussed around capping by comparison to costs would also apply to capping egress fees by reference to other charges.

W.167 We consider there to be substantial design risk in defining and determining the relevant benchmark fee to set an egress fee cap to, as well as greater monitoring and enforcement risk and regulatory burden. Cloud providers commonly have numerous different data transfer fees (for example, different internal data transfer fees depending on whether the transfer is going between zones, regions, countries, continents etc, or depending on the cloud product being used) and services are not always consistent and comparable between cloud providers.

W.168 There is also circumvention risk in setting a price cap by reference to another fee which can be changed by cloud providers, for example to bring the reference fee to current egress price levels. This would also lead to a distortion in the reference fee itself, which would cause other customers to pay more for the reference service. The potential circumvention risk is also likely to be higher if the reference service is a smaller or lesser used service, which could be the case if choosing one data transfer reference fee out of many options.

Cloud providers in scope

W.169 An egress fees remedy could:

(a) include all cloud providers;

(b) set a minimum size threshold (eg set by reference to revenue) and include all cloud providers above that threshold; or

(c) be limited to cloud providers which have significant market power.

W.170 We consider that there could be benefit in targeting the remedy at a small number of larger providers above a particular threshold, and in particular, that an effective remedy could be achieved by focusing any remedy on the largest cloud providers. This is because:

(a) the cloud services market is concentrated, for example AWS and Microsoft have a combined market share (IaaS and PaaS) of 60-70% (and 80-90% of IaaS market).[95] Therefore, the majority of customers in the cloud services market would benefit directly from a remedy that covered at least the two larger providers; and

(b) a remedy which targeted the largest providers would directly and indirectly constrain egress fee charges for cloud customers, including by changing the commercial conditions in the wider sector. For example:

(i) Following the introduction of free ingress by Microsoft, other providers followed suit which has resulted in data ingress now typically being free with all major cloud providers.[96]

(ii) There is evidence that suggests that AWS, Microsoft and Google do often consider and/or follow each other's pricing changes.[97]

(iii) For changes to egress specifically, we have seen evidence in an internal document that a cloud provider specifically considered removing egress fees, but was concerned that others would easily do the same.[98]

(iv) AWS said that one of the reasons behind why it made its decision to provide free switching egress in part as it [✂].[99]

Egress services and transfers in scope

Routing options included

W.171 One of the key design considerations for this remedy is defining the egress data transfers that are to be covered by the potential remedy. Cloud providers use

[95] Shares of supply are by reference to revenue, see Chapter 3 [market shares].
[96] Ofcom Cloud services market study final report, paragraph 11.33 and footnote 1179.
[97] For example, AWS and Microsoft followed Google in introducing global free switching programmes. [✂]. Responses to the CMA's information requests [✂].
[98] [✂] response to the information request [✂].
[99] Note of meeting with AWS [✂].

different terminology for egress,[100] and a potential remedy would need to ensure that it was well specified for the companies in scope.

W.172 We consider that a potential remedy should include the full range of egress transfer services, particularly in order to minimise potential for circumvention, and so it should cover all routing options. In particular we note that:

(a) Limiting the scope to ISP routing, as submitted by Microsoft, risks degradation of, or distortions to, the service;[101] and

(b) The 'premium' characteristics of backbone network routing (eg higher reliability and resiliency, lower latency) may be necessary for customers to effectively multi-cloud.

W.173 However, while we consider that egress data transfers via any routing option could be within scope, there are reasons that customers' direct connections and transfers from a content delivery network (CDN) services should be excluded. In particular:

(a) Direct connections: We recognise that customer direct connections tend to be used for more specialised customer use cases and/or be for transfers to on-premises infrastructure, and as such a customer would not necessarily be comparing these services to the regular egress services of another cloud provider. Furthermore, the risk that the direct connections exception may be unclearly specified or able to be used to circumvent the remedy is low, as our understanding is that direct connections require the build and set up of dedicated physical interconnection infrastructure between each customer and the cloud provider at supported sites. This means that there is identifiable infrastructure to tie this exception to, as well as a cost disincentive to cloud providers and customers to use direct connections instead of internet egress under this remedy.[102]

(b) CDNs: Our understanding is that customers primarily use CDNs to deliver content to end users or applications, and so egress data transfers from a CDN would not be likely to be for switching or multi-cloud use. Furthermore, CDNs are a distinct service and appear to be consistently defined and well-specified across most cloud providers.

W.174 Whilst AWS, Microsoft and Google have submitted that they will have reduced incentive to invest in providing a premium network if egress fees were capped or

[100] For example, AWS uses the term 'data transfer out ('DTO'), Oracle sometimes uses the term 'data mobility' and Google refers to inter-region and inter-zone data transfers as 'transit egress'.
[101] For example, our review of Google's internal documents [✂]. Google's response to the information request [✂].
[102] Direct connections are also typically more expensive than using egress data transfer services, unless a customer has very high egress usage.

banned,[103] we consider this distortion risk to be low given that network quality is important to a cloud providers' offering for many other cloud services which would reduce any incentives to degrade this offer particularly where egress revenue is a small proportion of the total revenue associated with this network.

Identifying switching / multi-cloud egress transfers

W.175 Customers may seek to move their data out of a cloud provider's environment for numerous reasons, potentially incurring egress fees in the process. The customer detriment we have provisionally identified relates to egress fees arising from barriers to switching and/or multi-cloud, and so a remedy aimed at addressing this concern should be targeted at those egress data transfers associated with switching and multi-cloud.

W.176 Cloud providers have said that they cannot determine the purpose of data transfers.[104] However, we consider that specifying the type of egress in scope based on destination would appear a suitable alternative to identify those transactions being used for switching and/or multi-cloud purposes, and so a potential remedy should be focused on egress data transfers between public clouds ('cross-cloud egress').

W.177 Cloud providers have also said that they cannot consistently identify the company and/or the relevant business unit/subsidiary within that company to which data is transferred and whether the peer is the end destination.[105] However, we understand that customer self-attestation may be an option for identifying relevant data transfers, and we observed it is currently used for AWS', Microsoft's and Google's free switching programmes and by IBM for compliance with current EU Data Act requirements.[106] We also recognise that this may have practical challenges for ongoing multi-cloud use by customers.

W.178 Alternatively, ASNs or other methods may potentially be used to identify cross-cloud egress.[107] To the extent that this may capture excess egress beyond switching and multi-cloud egress, noting that some cloud providers have raised issues with the use of ASNs, we note that this would incentivise cloud providers to develop more accurate systems for classifying data transfers.

W.179 In relation to the concern raised by Google and another cloud provider that customers may not want cloud providers accessing destination information about

---

[103] AWS' response to the Updated issues statement and working papers, paragraph 32; Microsoft's response to the Competitive landscape, Committed spend agreements and Egress fees working papers, paragraph 9; Google's response to Egress fees working paper, paragraph 57 and Annex response (h).
[104] Responses to the CMA's information requests [✂].
[105] Responses to the CMA's information requests [✂].
[106] Amazon EC2 FAQs (accessed 30 October 2024); Cancel and delete your Azure subscription - Microsoft Cost Management - Microsoft Learn (accessed 30 October 2024); Google Cloud Exit free data transfer request (accessed 30 October 2024). [✂] response to the CMA's information request [✂].
[107] [✂]. Responses to the CMA's information requests [✂]. [✂].

their data transfers,[108] our understanding is that cloud providers already have some visibility over destination information from ASNs.[109]

Information transparency requirements

W.180 We consider that customers need to be aware of the effects of the potential remedy, ie that egress fees have been reduced or removed for switching and using multiple clouds. Without sufficiently clear information available to accurately forecast egress fees for switching and/or multi-cloud use, customers may be more reluctant to switch and/or multi-cloud. Absent this requirement, we would be concerned that affected companies would choose not to widely disclose the reduced egress fees.

W.181 Therefore, we consider there to be a benefit in including additional transparency requirements in an egress fees remedy, such as:

(a) A requirement to clearly display the level of egress fees applicable to cross-cloud transactions in a prominent and specific (ie unbundled) manner on their main public pricing pages;[110] and

(b) A requirement to clearly display the level of egress fees applicable to cross-cloud transactions in a prominent and specific (ie unbundled) manner on any private and/or personalised data transfer pricing pages for customers.

Interactions with other laws and regulations

W.182 The EU Data Act[111] entered into force in January 2024 and imposes obligations on cloud providers via provisions relevant to egress fees for EU customers. These obligations are explained in more detail in Chapter 6.[112]

W.183 The EU Data Act does not apply to UK customers, however it does require cloud providers to comply with requirements for egress pricing based on data transfer purpose.

W.184 In addition, since the start of the application of Article 29(2) of the EU Data Act, free switching programmes (ie programmes providing free egress for switching) have been voluntarily introduced globally by Google, AWS and Microsoft. We set out our assessment of these free switching programmes in Chapter 6 and Appendix N. In summary, we find that the programmes have limited and uncertain

[108] Google's response to Egress fees working paper, Annex response (e); [✂] submission to the CMA [✂].
[109] We also note that this potential customer concern has so far only been raised by two cloud providers.
[110] For example: EC2 On-Demand Instance Pricing - AWS; Pricing - Bandwidth - Microsoft Azure.
[111] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) ('EU Data Act').
[112] EU Data Act, Articles 29(1), 29(2), 29(3) and 34(2).

scope, including that they do not cover multi-cloud use, and do not materially affect the conclusions of our analysis of either switching costs or multi-cloud costs.

W.185 We consider that reliance on these programmes would not address the concerns provisionally identified. For example:

(a) The companies are not currently obliged to maintain these in the UK, so they could change at any time and we do not consider there to be a sufficiently strong reputational risk to cloud providers to ensure their continuation.

(b) They are also limited in scope compared to the design elements we discussed above, eg they exclude partial switching and multi-cloud, have time-limits on when switches must be completed, and can include restrictions on types of data or routing options.

(c) There is limited visibility which affects customers' awareness, something which is particularly acute given the requirement that customers actively apply for these programmes.

Monitoring and enforcement

W.186 As noted above, an egress fee ban would substantially reduce the level of monitoring work required as it would remove the need to calculate and monitor the fees being offered and applied to customers. A remedy which involved capping by comparison to cost, or by reference to other fees charged by the cloud provider may require more intrusive measures and/or be accompanied by a higher monitoring risk.

W.187 In terms of the information transparency requirement, this could be directly monitored through the main public pricing pages for cloud providers in scope and collect information on private customer pricing and egress fee billing periodically.

W.188 The inclusion of information transparency requirements would also allow customers and other market participants to be able to identify instances of non-compliance. The effect of this additional scrutiny would be dependent on stakeholders having good understanding of the allowed cost level, which again would be more apparent under a ban.

Effectiveness assessment

W.189 For the reasons discussed above, we consider that an effective remedy for egress fees could:

(a) Involve banning egress fees;

(b) Include at least AWS and Microsoft;

(c) Cover all egress transfer routes, except for direct connections and transfers from a CDN; and

(d) Include an information transparency requirement.

Expected impact on AEC and risk profile

W.190 Given the straightforward price methodology for a ban, this potential remedy is relatively simple to design, implement and monitor. For the reasons discussed above, this approach would minimise the specification, circumvention, distortion and monitoring and enforcement risks for this design element of the remedy.

W.191 Including at least AWS and Microsoft would directly and indirectly constrain egress fee charges for cloud customers, including by changing the commercial conditions in the wider sector. Whilst a market investigation order could also include other cloud providers, for the reasons we discussed in the 'Cloud providers in scope' section above we do not consider it to be necessary for this remedy to be effective.

W.192 Covering all egress transfer routes, with limited and well-specified exceptions, would also seek to minimise the potential for circumvention and distortions.

W.193 A pricing information transparency requirement would enhance the effectiveness of the remedy by making pricing information about the egress fees for switching and/or multi-cloud use clearly and readily available. This would result in customers being better informed when exercising choice and responding to offers.

Risks arising from under-recovery of egress costs

W.194 When assessing the design of potential remedies, we considered the risks and implications associated with under-recovery of egress costs, in particular around the potential that this may cause harmful distortions. This risk would be relevant for any form of egress fee price control but is particularly relevant to a ban.

W.195 As discussed above, we consider that any distortion risk arising from a reduced incentive to invest would be low given that network quality is important to a cloud providers' offering for many other cloud services. This would reduce any incentives to degrade this offer particularly where egress revenue is a small proportion of the total revenue associated with this network.

W.196 A restriction on affected providers from being able to recover costs through their customer base[113] also appears to be a relatively low risk given that:

[113] For example, Google's response to Egress fees working paper, paragraphs 3c) and 58-59; [✂] submission to the CMA [✂].

(a) Our analysis indicates that the large majority of the costs identified by cloud providers as incurred in relation to providing egress data transfers are for shared assets and shared operating and overhead (indirect) costs. These costs could justifiably be recovered through other networking service charges. Our analysis has identified internet transit (ie bandwidth) and peering costs to be the main egress-specific cost incurred by cloud providers. We found these egress-specific transit and peering costs to be relatively low value compared to the other costs submitted by cloud providers and/or compared to their cloud business cost bases overall.[114] In addition, larger suppliers have some settlement-free peering arrangements between [✂] in the UK which would mean peering costs would not apply to cross-cloud egress in many cases.[115]

(b) As generally the same assets are used to ingress and egress customer data,[116] we would expect the same arguments about potential distortion risks from lost cost recovery to apply to ingress data transfers. However, we have not seen evidence of distortions arising as a result of cloud providers making ingress free for customers.

W.197 For similar reasons, we consider the potential distortion risk of cloud providers having reduced investment and innovation under a ban or cap,[117] or increasing prices for other cloud services to recover costs,[118] to be limited.

W.198 Given the shared assets used in providing egress data transfer services and limited remedy scope of cross-cloud egress for UK customers, affected cloud providers would be able to use revenues from other types of egress and wider networking and cloud services to fund investment and innovation.

W.199 Potential price rises in other services seems unlikely to be a large distortion and we observe that AWS, Microsoft and Google have not appeared to increase other prices as a result of introducing free switching programmes,[119] and by the same logic cloud providers' decisions to make ingress free could have resulted in other price increases, which again we have not seen evidence of. The costs associated with cross-cloud egress for UK customers also seem unlikely to equate to

---

[114] CMA analysis of transit and other costs for AWS, Microsoft, Google, Oracle and IBM. Sources: Responses to the CMA's information requests [✂]; Form 10-Ks for Amazon, Microsoft, Alphabet, Oracle and IBM.
[115] See Appendix Q, Cloud providers' egress costs for further details of our analysis.
[116] Responses to the CMA's information requests [✂].
[117] As submitted by AWS, Microsoft and Google. AWS' response to the Updated issues statement and working papers, paragraph 32; Microsoft's response to the Competitive landscape, Committed spend agreements and Egress fees working papers, paragraphs 9 and 83; Google's response to Egress fees working paper, paragraph 57 and Annex response (h).
[118] AWS response to the Issues Statement dated 17 October 2023, paragraph 29; AWS' response to the Egress fees working paper, paragraphs 15 and 28; Microsoft's response to the Competitive landscape, Committed spend agreements and Egress fees working papers, paragraphs 97-99; Summary of hearing with Microsoft, paragraph 66; Microsoft response to the Issues Statement dated 17 October 2023, paragraph 61; Google response to the Issues Statement dated 17 October 2023, paragraph 30a); IBM's response to the Egress fees working paper, page 2.
[119] AWS and Google confirmed [✂]. Note of meeting with AWS [✂]; Note of meeting with Google [✂].

significant cost increases for customers if incorporated into other cloud service prices.

W.200 In relation to Microsoft's submission that banning egress fees will distort prices and undermine clarity and predictability of cloud spend for customers as there is no connection between customer consumption of the data transfer service and payment for the service, we consider that:

(a) A free egress data transfer service for cross-cloud egress (with transparent information) would be clearer and more predictable than a service with tiered fees (as currently exists); and

(b) Cloud providers offer other data transfer services for free, for example ingress and some types of internal data transfers. If price distortions due to lack of connection between customer consumption and payment for data transfer services was a likely risk for egress fees, we would expect to see distortions having arisen from free ingress and internal data transfer services. We are not aware of any material distortionary impacts arising from this.

W.201 AWS, Microsoft, Google and another cloud provider have also raised inefficient network usage or security risks arising from excessive egress usage as a potential unintended consequence if capping or banning egress fees.[120] As discussed in the egress fees chapter, we see these risks as limited for cross-cloud egress.

Monitoring compliance and enforcement

W.202 We considered the risks associated with monitoring and enforcement to be relatively low, given the limited scope and that a ban would be relatively straightforward to monitor (with the potential for extra scrutiny from other stakeholders).

Timescales

W.203 Where the CMA is taking action itself, the implementation of remedies following a market investigation typically involves the CMA making an order or accepting undertakings, which it must do within six months of the date of publication of the final report.[121]

W.204 We consider that there would not be a substantial implementation period following the imposition of the potential egress fees remedy given the pricing change for egress in scope and that the required updates to public and private pricing

[120] AWS' response to the Egress fees working paper, paragraph 17; Microsoft's response to the Competitive landscape, Committed spend agreements and Egress fees working papers, paragraphs 9 and 95; Google's response to the Egress fees working paper, paragraph 57 and Annex response (h); [✂] submission to the CMA [✂].
[121] The Act, Section 138A. The CMA may extend the six-month period only once and by up to a further four months if it considers that there are special reasons why a final order cannot be made within the statutory deadline.

information would not require substantial time to change. There are some elements which may take longer, in particular we recognise that developing or refining more automated methods of identifying cross-cloud egress may take some time, however at a minimum identification via customer self-attestation would be capable of timely implementation given this is already being used.

Interactions with other laws and regulations

EU Data Act

W.205 We have considered whether there is a tension between our potential remedy and the EU Data Act.

W.206 The EU Data Act only applies to EU customers and not UK customers.[122] In addition, the removal of egress fees for switching would be consistent between the EU and UK, and if any companies choose to remove egress fees for multi-cloud in the EU to align with the UK they would likely be compliant with the 'cannot exceed costs incurred' provision of the EU Data Act for in-parallel use.[123] Therefore, this remedy would not appear to be in conflict with obligations on cloud providers under the EU Data Act.

W.207 We also note that the risk of tensions arising from different pricing requirements between the UK and EU to be limited, given that cloud providers already use different regional pricing.

Implementing an egress fees remedy using the markets investigation powers

W.208 We consider that a ban on egress fees for switching and multi-cloud, applied to at least AWS and Microsoft, could, in principle, represent an effective standalone remedy to the egress fees feature we have provisionally identified. However, any egress fees remedy needs to be considered in the context of the wider remedial action we are proposing, specifically the recommendations to the CMA Board and our expectation that the CMA Board would act upon these in a timely manner.

W.209 We are concerned about the effectiveness of a remedies package that included our proposed recommendations to the CMA alongside an egress fees remedy using our remedy-making powers under the Act. These concerns would arise from a process of implementing, monitoring and maintaining any remedies implemented under the DMCC Act in parallel with an egress fees remedy under the Act, and the coherence of any substantive obligations being placed on AWS and Microsoft were the CMA to designate these parties with SMS status. In particular:

[122] EU Data Act, Articles 29(1), 29(2), 29(3) and 50.
[123] EU Data Act, Article 34(2).

(a) During any overlapping period between a remedy implementation phase using the remedy-making powers under the Act and any SMS investigations under the DMCC Act, AWS and Microsoft would be engaging with two separate parts of the CMA operating under different legal frameworks in relation to the same markets/activities. We consider that this would add considerable complexity associated with implementing remedies in these markets through these two regimes.

(b) Although we consider the risks associated with monitoring and enforcement of an egress fee remedy (in particular a ban) to be relatively low, the ongoing monitoring and enforcement of such a remedy alongside parallel monitoring and enforcement of any potential obligations imposed on AWS and Microsoft under the DMCC Act, would increase ongoing complexity. This approach would also raise a risk of contradictory or conflicting obligations and/or approaches to monitoring and enforcement by the CMA.

(c) Any increased regulatory complexity could undermine the effectiveness of interventions considered appropriate under the DMCC Act. The implementation and enforcement of interventions through the market investigation could reduce the flexibility available to the CMA to design and implement a complete and holistic set of effective interventions following any SMS designation.

W.210 We also consider that implementing and maintaining a remedy using our remedy-making powers under the Act in parallel with the CMA exercising its powers under the DMCC Act in respect of AWS and Microsoft in the same markets/activities could be an inefficient use of CMA resources, particularly given there is an overlap between the remedial powers in the two regimes.

W.211 In view of the above, we consider that implementing an egress fees remedy using our remedy-making powers under the Act would introduce risks to an overall remedies package that included our proposed recommendations to the CMA Board, and this would risk undermining the effectiveness of the remedies package as a whole.

W.212 These risks would not arise were the CMA to consider the imposition of appropriate interventions to address egress fees following any SMS designation of AWS and/or Microsoft in respect of cloud services. We consider that if the CMA were to designate AWS and Microsoft with SMS in respect of cloud services it would have the ability to impose appropriate interventions to address egress fees such as those identified in this report.

Other potential remedies

W.213 The final potential remedy that we consulted on was an increase in the visibility and clarity of egress fees for customers, potentially as part of wider requirements on providers to improve the predictability of, and customers' ability to control, their spend on cloud.

W.214 We have not received significant comments from parties in relation to an information transparency remedy for egress fees. AWS and Google submitted that an information transparency intervention was unnecessary, whilst IBM submitted that an information transparency remedy would be sufficient to address any perceived issues with egress fees, without the need for stronger price control remedies.[124] We received some comments from Oracle in favour of requiring cloud providers to adopt standardised terminology and display egress fee prices prominently on webpages and/or in contracts[125] and Vodafone submitted that cloud providers could facilitate an independent third party to provide comparison data.[126]

W.215 As we have not found that predictability of egress spend is an underlying feature of our provisional AECs[127] we have not considered an information transparency remedy of this nature to be necessary.

W.216 However, we have discussed the role of information transparency requirements in the potential remedy above, to support its effectiveness.

Microsoft's licensing practices

W.217 In this section, we set out our views on three potential remedies to the AEC we have provisionally found relating to Microsoft's licensing practices. We have structured the section as follows:

(a) first, we describe these potential remedies;

(b) second, we set out stakeholder views;

(c) third, we set out an analysis of these potential remedies, in particular focusing on the design considerations and risk profiles;

(d) fourth, we set out our views on the package of remedies and our views on its effectiveness; and

[124] AWS' response to the CMA's Egress fees working paper, paragraph 31; Google's response to Egress fees working paper, Annex response (i); IBM's response to Egress fees working paper, pages 1-2.
[125] Oracle's response to the Updated issues statement and working papers, pages 2-3.
[126] Vodafone's response to working papers, page 2.
[127] See Chapter 5, Egress Fees.

(e) finally, we discuss other potential remedies.

Description of potential remedies

W.218 We considered three potential remedies to address the AEC we have provisionally found relating to Microsoft's licensing practices and the five software products which we have focused on, namely Windows Server (which includes Active Directory functionality), SQL Server, Windows 10/11, Visual Studio and Microsoft productivity suites.

W.219 These three potential remedies are:

(a) Remedy A – Fair, reasonable and non-discriminatory pricing: This potential remedy would require Microsoft to apply a 'FRAND' approach in relation to pricing its Software products regardless of which cloud they are hosted on.[128] It would also include information transparency obligations.

(b) Remedy B – Product functionality and technical performance: This potential remedy would impose restrictions on Microsoft's ability to favour its own cloud through licensing practices which grant unequal access to Software products and product functionality depending on which cloud the Software products are deployed on.

(c) Remedy C – Licence transfer: This potential remedy would focus specifically on contractual licensing practices relating to the transfer and/or deployment by end customers of previously purchased Software products on the cloud of their choice.

W.220 These potential remedies would apply to all the products set out above, together with related services which support the deployment of those Software products for use on cloud (eg extended security updates).

W.221 Given the ongoing development of Microsoft's portfolio of software products, we consider that these potential remedies would need to cover any future versions of these products, and/or functionally similar products available for deployment on a public cloud, to manage potential circumvention and specification risks.[129]

Stakeholder views

W.222 In our Licensing working paper, we considered the following three potential remedies relating to Microsoft's licensing practices, plus a separate information

[128] A FRAND approach would require Microsoft to provide access to its software products on fair, reasonable and non-discriminatory pricing terms, where different fees and commercial terms are charged to different customers only where objectively justified.
[129] See Chapter 6.

transparency remedy which has subsequently been incorporated into Remedy A above:[130]

(a) non-discriminatory pricing for Microsoft software products, regardless of which cloud they are hosted on;

(b) allowing customers to transfer previously purchased Microsoft software products to the cloud of their choice without additional cost; and

(c) requiring parity of Microsoft software products and product functionality for use on Azure and non-Azure cloud.

W.223 Several stakeholders[131] commented on the design and effectiveness of the overall package of remedies put forward by the CMA in its Licensing working paper, including the benefits of including remedies targeted at non-pricing licensing practices as well as pricing practices.[132] For example:

(a) AWS said that it is important for remedies which address licensing practices to go beyond pricing constraints, to other factors which can significantly impact customer choice of IT provider for running Microsoft workloads;[133] and

(b) a stakeholder told us that it was concerned about potential circumvention risks associated with price-related remedies relating to Microsoft's ability to discriminate on price by tweaking some of the technical features of the product (eg virtual machines; windows software). It submitted that the challenge is in part that there may be a non-price factor which effects a price difference, but that may not be charged as a price difference.[134]

W.224 One cloud provider told us that licensing remedies should include the removal of the concept of Listed Provider (or any equivalent concept), because this would be necessary for ensuring a level playing field. It submitted that this would be straightforward to implement, without the need for any technical changes or ongoing monitoring requirements by the CMA, and that [✂].[135]

W.225 One cloud provider told us that licensing remedy design should include a general provision requiring Microsoft to negotiate in good faith and provide access to software products for resale to any third party cloud providers under any Licensing Agreement on fair, reasonable and non-discriminatory terms.[136]

---

[130] Licensing working paper, paragraph 7.5.
[131] Submissions to the CMA [✂]; Note of meeting with [✂].
[132] We have also received stakeholder feedback relating to the design and effectiveness to the individual remedies we set out in the Licensing working paper, which we comment on below when setting out our views on the three potential licensing remedies we have considered.
[133] AWS' submission to the CMA [✂].
[134] Note of meeting with [✂].
[135] [✂] submission to the CMA [✂].
[136] [✂] submission to the CMA [✂].

W.226 In relation to the specification of an overall package of licensing remedies, one cloud provider submitted that:

(a) software products should be defined to include any existing or future versions of software licences for those products included in the remedy, or any future name by which those products are known, as well as any software licences for software released after the date of the remedy being introduced, performing materially the same function as the software listed;[137] and

(b) the remedy provisions should not be specific to BYOL and SPLA constructs that exist today, but should cover any practices or contractual requirements that have the same effect as these.[138]

W.227 In terms of overall approach, CCIA told us that licensing remedies will need to:

(a) address customers that are already experiencing some degree of lock-in, not only those customers that might experience lock-in in the future;[139] and

(b) address the range of means by which licensing terms for legacy software can restrict the choices of customers in ways that either directly or indirectly (by impeding their ability to choose alternatives) raise quality-adjusted prices. CCIA told us that if only some of those means are limited, this may simply lead to other restrictions being used to extract the same rents.[140]

W.228 A stakeholder submitted that any remedies in relation to Microsoft's licensing practices should encompass the licensing practices of other cloud providers.[141] As remedies would be aimed at addressing the AECs that we have provisionally found, and we have not investigated other providers' licensing practices, we do not consider that the scope of the remedy should be extended to other cloud providers' licensing practices.

W.229 One academic[142] told us that the adoption of FRAND commitments, in addition to transparency, could mitigate concerns identified in the Licensing working paper relating to Microsoft's licensing practices, but that implementing measures such as prohibiting the granting of discounts to users of a firm's software operating on its cloud unless the cloud also extends same reductions to its competitors will likely result in higher prices for businesses in the UK.

---

[137] [✂] submission to the CMA [✂].
[138] [✂] submission to the CMA [✂].
[139] CCIA response to the Licensing working paper dated 06 June 2024.
[140] CCIA response to the Licensing working paper dated 06 June 2024.
[141] Open Cloud Coalition Position Paper on the CMA Cloud Services Market Investigation. Members of Open Cloud Coalition include Google Cloud.
[142] R. Parisi, The Cloud Services Markets' Competitive Landscape: A contribution to the Competition and Markets Authority.

Stakeholder views on principles-based remedy design

W.230 In the Licensing working paper we invited views from stakeholders on the role of principles-based remedies in relation to Microsoft's licensing practice.[143]

W.231 AWS, a cloud provider, CFSL and CISPE told us that there are benefits in using principle-based remedies in relation to Microsoft's licensing practices.[144]

W.232 SMF said that adherence by cloud providers to principles for fair software licensing in cloud, including the freedom to bring previously purchased software to the cloud could help mitigate the impact of restrictive licensing practices.[145]

W.233 CCIA told us that it considers that these remedies might be most effective with a mix of specific requirements (to spur immediate action) and principles (to avoid workarounds that undermine the effectiveness of the intervention).[146] However, CCIA also submitted that even if the principles are not there, they are still implicit in the practices the specific interventions are targeted at.[147]

W.234 AWS,[148] CISPE[149] and CCIA[150] also submitted that the design of underlying principles relating to Microsoft's licensing practices could be based on the Ten Principles of Fair Software Licensing published by CISPE and Cigref in 2021,[151] which include for example:

(a) equal treatment for software licensing fees in the cloud; and

(b) freedom to bring previously purchased licences to the cloud.

W.235 A cloud provider submitted that although it considers that Microsoft's conduct should primarily be remedied through the imposition of clearly defined rules, it agrees with the CMA's suggestion that supplementing such rules with enforceable principles-based remedies could help avoid circumvention risk.[152]

W.236 A cloud provider told us that the remedy should include an overarching principle which places a general obligation on Microsoft not to unduly discriminate against third party cloud infrastructure services providers, such as to place them at a competitive disadvantage.[153]The cloud provider also told us that a benefit of

---

[143] Licensing working paper, paragraph 7.71.
[144] AWS Response to the Issues Statement dated 17 October 2023, paragraph 33; [✂] submission to the CMA [✂]; CFSL's response to the Issues Statement dated 17 October 2023, page 31; CISPE Response to the Issues Statement dated 17 October 2023, page 5.
[145] Social Market Foundation - clearing the air confronting the cost to cloud adopters of restrictive software licensing practices, page 8.
[146] CCIA response to the Licensing working paper dated 06 June 2024, page 3
[147] Note of a meeting with CCIA [✂].
[148] AWS Response to the Issues Statement dated 17 October 2023, paragraph 33.
[149] CISPE submission to the CMA [✂].
[150] CCIA response to the Licensing working paper dated 06 June 2024, page 1.
[151] Principles of Fair Software Licensing for Cloud Customers - Fair Software Licences last accessed 19 November 2024.
[152] [✂] submission to the CMA [✂].
[153] [✂] submission to the CMA [✂].

including an overarching principle is that it would restrict discrimination between cloud providers only to the extent that it is undue and places competing providers at a competitive disadvantage, and that a remedy which is limited to reversing only the most egregious aspects of Microsoft's current policies and practices would create significant risk of circumvention.[154]

W.237 A customer stated that remedies to address barriers to switching, including in relation to software licensing, could and should be addressed through Conduct Requirements.[155]

Stakeholder views on implementation, monitoring and enforcement

W.238 Several parties commented on implementation, monitoring and enforcement of potential remedies:

(a) AWS submitted that the majority of the remedies set out in the CMA's working paper could be easily implemented through simply eliminating arbitrary and unfair contractual restrictions, rather than requiring technical changes, as is shown by Microsoft's 2022 changes [✂]. [156] For example, AWS told us that it considers Microsoft should be able to offer a remedy relating to product availability and product functionality without making technical changes, since Azure customers already receive all the requested benefits.[157]

(b) a cloud provider told us that it considers these remedies would be readily capable of effective monitoring and enforcing,[158] and provided an example of how they could be monitored through the use of a Monitoring Trustee (at Microsoft's cost).[159]

(c) CCIA submitted that remedies should be simple from the customer's perspective and will ideally not require extensive negotiation or legal action by individual cloud customers.[160]

(d) CISPE publicly states that its own principles 'have been developed as an auditable best practice framework for businesses looking to the Cloud for growth, innovation and flexibility',[161] and has told us that it has developed a

[154] [✂] submission to the CMA [✂].
[155] [✂] submission to the CMA [✂].
[156] [✂] submission to the CMA [✂].
[157] [✂] submission to the CMA [✂].
[158] [✂] submission to the CMA [✂].
[159] [✂] submission to the CMA [✂].
[160] CCIA response to Licensing working paper dated 06 June 2024, page 1.
[161] Principles for Fair Software Licensing in the Cloud | CISPE - The Voice of Cloud Infrastructure Service Providers in Europe, last access on 19 November 2024.

comprehensive control and testing framework, relating to the real application of the Principles of Fair Software Licensing for Cloud customers.[162]

W.239 One customer and Google also commented on routes to implementation:

(a) the customer submitted that, as the DMCC Act gives the CMA power to set conduct requirements for SMS firms to ensure they do not have an adverse effect on competition, the types of remedies the CMA is considering, including in relation to software licensing, could and should be addressed through these.[163]

(b) Google favoured implementing remedies relating to Microsoft's licensing practices through a market investigation order: it submitted that it is generally appropriate for the CMA to consider whether the DMCC Act would be an appropriate tool to address competition issues resulting from substantial and entrenched market power in the relevant market, but considers that, in the context of Microsoft's anti-competitive licensing practices and related technical barriers, it would be more appropriate for the CMA to use its existing market investigation remedy powers to address harm relating to Microsoft's licensing practices and related technical barriers (ie interoperability of Microsoft's IAM tools).[164] Google also said that it considers that the licensing practices concerned are easily remediable under the CMA's market investigation powers, and that there is a need for urgent remedial action to be taken to prevent further damage to competition in the cloud services market at a critical inflection point.[165]

Microsoft's views

W.240 Microsoft told us that there is no actionable 'discrimination' to remedy, that it is justified in treating smaller cloud providers differently, and that in mandating the application of equivalent terms to dissimilar transactions with dissimilar counterparties, a non-discriminatory pricing remedy would introduce harmful discrimination in the name of removing it.[166]

W.241 Microsoft submitted that imposing remedies in respect of Microsoft's intellectual property (IP) in the context of this market investigation would be unprecedented, because the UK would be regulating IP licensing terms that are not the subject of any current regulation or enforcement action in the US, EU or indeed any other jurisdiction (unlike, for example, egress fees under EU rules).[167]

---

[162] CISPE submission to the CMA [✂].
[163] [✂] submission to the CMA [✂].
[164] Google's submission to the CMA [✂].
[165] Google's submission to the CMA [✂].
[166] Microsoft's submission to the CMA [✂].
[167] Microsoft's submission to the CMA [✂].

Analysis of the three potential remedies

W.242 In this section we set out an analysis of the three potential remedies we described above. We discuss the design of each of the potential remedies individually, before turning our minds to their overall effectiveness as a package of remedies.

W.243 We consider that a package of potential remedies would likely need to consist of a combination of high-level principles and rules-based interventions. This is because targeted rule-based provisions would provide clarity to Microsoft and third parties on how certain obligations would be implemented in practice, and ensure they are capable of being effectively monitored and enforced. The inclusion of high-level principles would manage the circumvention risks inherent in applying rules-based provisions while allowing Microsoft some greater degree of flexibility in how it would comply with aspects of the remedy on an ongoing basis.

W.244 For this reason, we consider that a package of remedies including both rules-based and principles-based obligations would be required to comprehensively address the harm identified from Microsoft's licensing practices. In the following section, we set out the design considerations for each of the constituent elements of this possible remedies package.

Remedy A: Fair, reasonable and non-discriminatory pricing

Description of remedy and intended effect

W.245 The first of the inter-related potential remedies that we have considered was a restriction on Microsoft's use of licensing practices relating to the pricing of its software products, which we have provisionally found to contribute to an AEC.

W.246 The aim of this potential remedy would be to address Microsoft's ability to favour its own cloud services compared to those of its rivals through licensing practices which, either directly or indirectly, make its software products more expensive when used with rival cloud services compared to Microsoft's Azure services, and prevent equivalent conduct arising in the future.

W.247 As set out in more detail below, we consider this remedy should be designed using a FRAND-based approach, requiring Microsoft to provide access to its software products on fair, reasonable and non-discriminatory terms, where different fees and commercial terms are charged to different customers only where objectively justified.

W.248 We envisage that this potential remedy would comprise:

(a) a high-level principle requiring Microsoft to apply a FRAND approach in relation to pricing its software products, regardless of which cloud they are hosted on;

(b) a non-exhaustive list of targeted, rules-based provisions setting out how this principle should be implemented in relation to Microsoft's existing licensing practices; and

(c) information transparency obligations, requiring Microsoft to publish clear and transparent information relating to the FRAND-based pricing of its software products across Azure and non-Azure clouds.

W.249 The scope of this remedy would include addressing Microsoft's contractual policies and pricing structures which are capable of directly or indirectly raising the relative cost to customers of using Microsoft software products on non-Azure clouds compared with on Microsoft's own cloud, including for example through discounting structures such as AHB.

Stakeholders' views

W.250 We have received a number of submissions on the design and effectiveness of potential pricing remedies.

W.251 Several stakeholders have commented on potential circumvention risks and specification risks relating to non-discriminatory pricing remedies, and how these could potentially be overcome through the design of the remedy.

W.252 For example:

(a) one cloud provider submitted that the following additional factors should be included in non-discriminatory remedies to manage circumvention risk, and that non-discriminatory remedies should:

(i) include the pricing of ancillary rights and features (not limited to but including ESUs,[168] Dual Usage rights and Failover rights); and

(ii) prohibit Microsoft from implementing contractual policies or pricing structures which are capable directly or indirectly of raising the cost of software licences based on the cloud infrastructure on which those licences are deployed (eg rebate schemes) and imposing fee structures via SPLA which are less advantageous than available to its own customers ([✂]).[169]

(b) CCIA[170] commented on circumvention risks if Microsoft is able to continue to charge for Software Assurance in relation to licence transfer. For example, CCIA submitted that there is a circumvention risk that Microsoft could comply with a narrowly defined price-based remedy but could then require customers

[168] Extended Security Updates.
[169] [✂] submission to the CMA [✂].
[170] CCIA response to Licensing working paper dated 06 June 2024; Note of a meeting with CCIA [✂].

to buy other products such as software assurance (ie software assurance is an example of a mechanism that could be used for varying cost if someone wanted to circumvent a price-based remedy).[171]

(c) Google told us that Microsoft should be required to immediately reverse a forward-looking August 2022 announcement that imposed new contractual terms on managed service providers (in particular those who do not have their own data centre capacities) with effect from October 2025 which differentiate between the pricing framework that applies to managed services providers, depending on whose cloud their Microsoft software products are hosted;[172] and

(d) a third party told us that one of the ways that Microsoft could potentially circumvent licence transfer remedies would be to implement a policy of not allowing BYOL of software to shared platforms.[173]

W.253 CCIA submitted that there are two main categories of circumvention risks:

(a) Microsoft adheres to any price requirement but requires other providers to use the software in a certain way, which does not represent the most efficient way for the other cloud provider to operate (eg requirements to host certain software on dedicated hardware); and/or

(b) Microsoft adheres to any price requirement for the services in scope but bundles the services in scope with other services that the other cloud provider may not require, and/or may not need to buy in another setting (eg on premises), which is where CCIA sees Software Assurance as an example.[174]

W.254 CCIA also submitted that notwithstanding these potential routes for circumvention, a remedy that addresses some of the concerns that its members have with Microsoft's licensing practices is still likely to be helpful, and that remedies do not need to perfectly address the practices to be effective.[175]

W.255 With regard to the risk that remedies which impose changes to 'wholesale' pricing structures (eg SPLA pricing for Listed Providers or non-Listed Providers), one cloud provider submitted that competitive pressures should prevent the addition of a significant margin, and that Microsoft would be incentivised to keep the gap between its wholesale and retail prices small to prevent its competitors from making a large margin.[176]

---

[171] Note of a meeting with CCIA [✂].
[172] Google's response to the Licensing working paper dated 06 June 2024, paragraph 47.
[173] CISPE submission to the CMA [✂].
[174] Note of a meeting with CCIA [✂].
[175] Note of a meeting with CCIA [✂].
[176] [✂] submission to the CMA [✂].

W.256 With regard to the risk of prices for Microsoft's software products going up rather than down in response to a non-discriminatory pricing remedy, AWS told us that Microsoft already has discretion to identify someone as a Listed Provider, effectively driving up costs for running Microsoft products on the provider they choose to designate.[177]

Stakeholder views on pricing methodology

W.257 In the Licensing working paper we invited views from stakeholders on potential methodologies that could be applied to a non-discriminatory pricing remedy relating to Microsoft's licensing practices.[178]

W.258 One cloud provider told us that it supports an approach that restricts Microsoft from charging materially different prices on a per-product basis, regardless of whether they are Azure end-customer prices or 'input prices' for non-Azure cloud providers.[179] It told us that non-discriminatory pricing remedies should include specific provisions prohibiting Microsoft from imposing wholesale prices for licences to third party cloud providers higher than retail prices it charges its own customers, as well as prohibiting Microsoft from charging different wholesale prices between third party cloud providers for the same software product, and that this form of remedy would not be difficult to implement from a practical perspective.[180]

W.259 CCIA told us that there are merits in simplicity, and that FRAND is always intensive in terms of the effort involved to get to a clear position on price. CCIA submitted that pairing a simple approach from a customer perspective, such as prohibiting wholesale price discrimination, with a principles-based approach could be the mix that would achieve the right answer.[181]

W.260 CISPE told us that it considers price parity remedies may need to include parity on a case-by-case basis because there are so many different configurations for customers using Microsoft software products, and said there should be a third party that identifies where there is discrimination.[182]

W.261 One cloud provider told us that a non-discriminatory pricing remedy would need to take into consideration that there may be additional costs, support risks and licensing compliance risks depending on the cloud a software product is deployed on that may justify some price divergence.[183] It told us that if Microsoft is selling a product allowing it to be deployed on a cloud other than Azure, it may be justified

---

[177] AWS' submission to the CMA [✂].
[178] Licensing working paper, paragraph 7.57.
[179] [✂] submission to the CMA [✂].
[180] [✂] submission to the CMA [✂].
[181] Note of meeting with CCIA [✂].
[182] Note of meeting with CISPE [✂].
[183] [✂] submission to the CMA [✂].

that the cost would be higher, but that it should not make a difference whether that product is sold by a Microsoft reseller that is also a cloud competitor or a reseller that is not.

Stakeholder views on information transparency

W.262 One of the potential remedies that we included in our working paper was an information transparency obligation,[184] which we have subsequently incorporated into Remedy A.

W.263 Oracle told us that it is in favour of increased transparency in relation to the use of Microsoft products on third party cloud infrastructure, but that increased transparency should apply across the board for all cloud competitors, citing Jigsaw Research findings that some customers find that cloud provider pricing and billing is complex and lacking in transparency.[185]

W.264 AWS told us that an information transparency remedy could help ensure that Microsoft cannot unfairly charge some customers more than others for its products, but only if introduced in conjunction with pricing remedies.[186]

W.265 CCIA submitted that unless accompanied by remedies which address also discriminatory pricing, this form of remedy could reinforce rather than mitigate the impact of those licensing practices.[187]

W.266 One cloud provider told us that although it does in principle support this form of remedy as part of a package of remedies, it considers that it would need to be carefully thought through to avoid unintended consequences.[188]

W.267 One third party told us that an audited-based approach would potentially be more effective for ensuring compliance with non-discriminatory pricing obligations than an information transparency remedy.[189]

Microsoft's views

W.268 Microsoft submitted that, as a non-discriminatory pricing remedy would require that pricing on Azure and every other cloud and every on-premises customer licence be the same, it would seem to provide that either Microsoft has to change Azure to sell only perpetual licences based on physical hardware or only vcore subscription licenses.[190]

---

[184] Licensing working paper, paragraphs 7.54-7.56.
[185] Oracle's submission to the CMA [✂].
[186] AWS' submission to the CMA [✂].
[187] CCIA response to Licensing Working paper dated 06 June 2024.
[188] [✂] submission to the CMA [✂].
[189] Note of meeting with [✂].
[190] Microsoft' submission to the CMA [✂].

W.269 Microsoft also submitted that a non-discriminatory pricing remedy in the form set out in our Licensing working paper would soften competition on the basis that:

(a) it would serve to level out what Microsoft describes as a relatively modest competitive advantage for the non-Listed Providers (the Flexible Virtualisation Benefit) to the benefit of AWS and Google; and

(b) to the extent that it limits the ability for Microsoft to discount, this reduces competition between Microsoft and Google/AWS and results in worse outcomes for UK customers.[191]

W.270 Microsoft further submitted that if one were to proceed down the intervention road of levelling out competitive advantages between differentiated suppliers in a differentiated market, then the thought experiment logically takes the regulator to odd places because levelling out one competitive advantage (that favours the IP creator, Microsoft) while leaving a host of others (that favour AWS, Google, Oracle, etc) would be manifestly distortive of competition.[192]

W.271 In relation to information transparency remedies, Microsoft submitted that there is already significant information transparency in relation to the pricing of its software products, and that any information transparency obligations should apply not only to Microsoft but also to AWS and Google.[193]

CISPE Settlement with Microsoft

W.272 In July 2024, CISPE announced that it had reached an agreement with Microsoft related to its competition complaint filed against Microsoft with the European Commission in November 2022. CISPE stated, that under a Memorandum of Understanding (MOU) signed by both parties, Microsoft had committed to make certain changes to address the claims made by European CISPE members and, as a result, CISPE would withdraw its complaint against Microsoft.[194]

W.273 According to CISPE, [✂]. We understand from CISPE that Listed Providers are excluded from the settlement so their concerns remain.[195]

Design considerations

W.274 In this section we discuss the key design considerations for a FRAND pricing remedy, setting out how this remedy could potentially be implemented using the CMA's market investigation powers, while seeking to manage the inherent

[191] Microsoft's submission to the CMA [✂].
[192] Microsoft's submission to the CMA [✂].
[193] Microsoft's submission to the CMA [✂].
[194] CISPE and Microsoft Agree Settlement in Fair Software Licensing Case, accessed 19 November 2024.
[195] Note of meeting with CISPE [✂].

complexity and circumvention risks of remedies targeted at Microsoft's licensing practices, including the fact that Microsoft is a vertically integrated firm.

W.275 We consider that any remedy design in this case would need to include provisions that address the different potential responses of Microsoft, in particular the scope for Microsoft to respond by (i) increasing its pricing of software products provided as an input to rivals and/or (ii) decreasing the prices charged to its own customers downstream.

W.276 In designing a remedy which seeks to control aspects relating to price, we consider that it would be necessary for this to include:

(a) a requirement to control prices which goes beyond focusing primarily on non-discrimination; and

(b) specification of how Microsoft would meet this requirement in practice.

Microsoft's transition to a subscription-based licensing model for public cloud

W.277 We have also considered the implications of Microsoft's transition to a subscription-based licensing model for public cloud on the remedy design. Chapter 6 sets out the relevant timeline and changes, the result of which was that customers can use the BYOL route to deploy certain Microsoft software on the public cloud of non-Listed Providers. However, customers cannot use the BYOL route to deploy any of their licences on Listed Providers' public or, with certain exceptions, on Listed Providers' private cloud.[196]

W.278 One effect of these changes was to introduce different pricing and contractual terms for Listed Providers and non-Listed Providers, which combines with Microsoft's wider transition to subscription-based licensing, and results in different routes and associated pricing structures being available to customers. This has the potential to increase the complexity of potential remedy design, with associated increases in risk.

Direct and indirect pricing mechanisms

W.279 The remedy design would need to take into consideration Microsoft's use of pricing and contractual structures which are capable of indirectly as well as directly impacting price, to manage potential circumvention.

[196] See Chapter 6 - Timeline of licensing practices.

W.280 As explained in Chapter 6, there are several pricing and contractual structures through which Microsoft could potentially raise the cost of using Microsoft's software products on rivals' clouds, compared to Azure, for example:

(a) differential pricing related to services which support the deployment of software products, without objective justification (eg on the basis of the cost of providing the service). This could include, for example, the Software Assurance benefits included in Microsoft's Software Assurance programme,[197] ESUs and other technologies, services and rights that customers may rely on to use Microsoft products efficiently and securely on the cloud of their choice;

(b) pricing for packages of products as well as individual products (eg Software Assurance); and

(c) pricing relating not only to the headline prices for the software products, but also to variations within tariffs and fee structures depending on which cloud the software products are hosted on, which are capable of raising the price of deploying those products on non-Azure cloud compared to Azure.[198]

W.281 To address these practices, we consider that this remedy would need to impose restrictions on pricing, contractual terms and fee structures for products, or packages of products (in some cases including supporting services – eg ESUs), which are capable of directly or indirectly raising the cost of deploying software products on non-Azure clouds compared with Azure.[199]

Pricing methodology

W.282 We consider that a key design consideration is the methodology for introducing pricing obligations in relation to Microsoft's existing licensing practices (and any equivalent conduct which arises in the future), in a way which are capable of being effectively implemented, monitored and enforced.

W.283 First, as discussed above, we consider it will be necessary for the design of this remedy to include a requirement to control prices which goes beyond focusing primarily on non-discrimination.

---

[197] Microsoft Volume Licensing - Microsoft Software Assurance, accessed on 18 October 2024.
[198] We consider this would include provisions targeted at contractual terms for existing products which we have identified as being capable of indirectly raising the price of Microsoft Software products on non-Azure cloud (eg free ESUs; Azure Hybrid Benefit; Windows 10/11 multi-sessions).
[199] Although the design of the overall licensing remedy includes separate provisions for price related licensing factors and non-price factors, we recognise that in practice most non-price factors will in some way impact on price and that there are therefore not always bright lines between what should be captured by non-discriminatory pricing obligations and remedy provisions relating to availability and functional equivalence of Software products. Therefore rule-based provisions targeted at non-price licensing practices may include also restrictions on how they are priced (eg ESUs).

W.284 Second, we consider that the remedy design would need to be capable of differentiating between pricing structures for customers which have previously purchased an on-premises Microsoft software product licence and who want to obtain the right to deploy that software product on the cloud, and those who do not have a pre-existing on-premises software product licence.

W.285 There are currently several different routes by which customers which have purchased an on-premises software product are able to deploy that software product on the cloud at a lower price than customers which have not previously purchased software licences. For example:

(a) since 2022, for the majority of Microsoft software products, customers are able to use the BYOL route[200] to deploy their on-premises Microsoft product licences on non-Listed Providers' public cloud provided that they have a relevant subscription licence or active Software Assurance;

(b) since 2022, for certain Microsoft software products, customers are able to use the BYOL route to deploy their on-premises Microsoft product licences on Listed Providers' public cloud provided that they have also purchased the relevant software subscription (eg SQL server); and

(c) according to Microsoft's website,[201] Azure Hybrid Benefit (AHB) allows customers with existing on-premises Windows Server or SQL Server core licences to migrate these licences onto Azure at a discount provided they have a relevant subscription licence or active Software Assurance.

W.286 Third, remedy design would need to provide for comparison of prices at different levels in the supply chain, given that Microsoft's direct customers on non-Azure clouds are, in some cases, other cloud service providers rather than the end-use customer.[202]

W.287 In view of the above, we consider that this remedy should be designed using a 'FRAND'-based methodology, requiring Microsoft to provide access to its software products on fair, reasonable and non-discriminatory terms, where different fees

[200] As explained in Chapter 6, BYOL is a term used when a customer relies on their on-premises Microsoft software product licence to deploy the Microsoft product on the cloud (whether Azure, third party, Listed, non-Listed, public or private).
[201] Azure Hybrid Benefit - Hybrid Cost Calculator - Microsoft Azure, accessed 19 November 2024. See Explore Azure Hybrid Benefit for Windows VMs - Azure Virtual Machines and Azure Hybrid Benefit - Azure SQL Database & SQL Managed Instance, accessed 19 November 2024.
[202] Microsoft's SPLA programme provides cloud providers with the right to integrate certain Microsoft products into their own cloud services and offer those cloud services to their end customers directly. The licence purchased under the SPLA covers the right to use the software on the hardware that the service provider uses to provide their services to their end customers. From Microsoft's perspective, the cloud provider is Microsoft's customer – the cloud provider pays Microsoft for its usage monthly in arrears based on how much Microsoft software the cloud provider actually used. In turn, the cloud provider charges its own end customer. SPLA is not a reseller programme for Microsoft software 'The routes to obtaining the right to use the Microsoft software' section of Chapter 6.

and commercial terms are charged to different customers only where objectively justified, rather than through a more straightforward price-parity obligation.

W.288 Specific consideration would need to be given to the basis on which the level of FRAND prices and terms would be set, and an appropriate oversight mechanism put in place. A commitment to permit access on FRAND terms would need to be sufficiently well specified such that Microsoft and third parties were clear on how it applied in practice, and to allow for effective monitoring and enforcement. It would also need to be responsive to future changes in Microsoft's contractual terms and pricing structures.

W.289 Furthermore, given the lack of direct comparability between some of the existing pricing structures and approaches, we consider that a pricing remedy would likely need to include rules-based provisions explaining how any pricing obligations are to be applied in relation to the contractual terms and charges currently in place (eg Software Assurance, AHB, SPLAs).

Information transparency

W.290 We considered that an information transparency obligation requiring Microsoft to provide more information on prices to end customers, in relation to the use of Microsoft software products on Azure and non-Azure clouds, is unlikely on its own to be an effective remedy. This is due to difficulties in identifying the breakdown of costs between resource and licensing components for cloud provider customers which would risk undermining the value of any information provided. Furthermore, often it may not be possible to give a true indication of the price of the software products to end customers – for example, the SPLA price is an intermediary price and may be incorporated (to differing extents) into the end price customers receive depending on decisions taken by their specific cloud provider, ie not Microsoft.

W.291 However, a more targeted information transparency obligation, focused primarily on the equivalence of the pricing Microsoft charges to its own customers, would likely be beneficial as part of a wider pricing remedy. The main intended benefit of this would be to enable some degree of monitoring by customers of the FRAND-based pricing requirements on Microsoft, by allowing them to compare the costs of hosting Microsoft software products on Azure and non-Azure cloud. We consider there would be benefit in being able to iterate the design of the information requirements to ensure they are sufficiently well-defined for monitoring purposes, in view of the inherent complexity in comparing the pricing of Microsoft's software products for use on different clouds as discussed above.

Remedy B: Product functionality and technical performance

Description of remedy and intended effect

W.292 The second of the inter-related potential remedies that we considered was a restriction on Microsoft's use of commercial practices that affect the technical performance of software products and product functionality depending on which cloud the software products are deployed on.

W.293 This remedy would seek to address Microsoft's use of non-price licensing practices which favour Microsoft's own cloud services by restricting availability of its software products and/or functionality of its software products on rival clouds. We would expect this to increase the contestable market by reducing the impact of non-price commercial practices, and in general minimise any differences in the technical performance of Microsoft software products when deployed on different clouds.

W.294 We considered that this potential remedy would comprise:

(a) principles-based obligations requiring Microsoft:

(i) to facilitate a consistent experience for customers who use Microsoft software products on Azure or non-Azure clouds, including in relation to product functionality, unless objectively justified; and

(ii) not to take measures which degrade the technical performance of a software product when deployed on non-Azure cloud relative to Azure, for example by withholding access to product functionality.

(b) a non-exhaustive list of targeted, rules-based provisions setting out how this principle should be implemented in relation to Microsoft's existing licensing practices.

Stakeholders' views

W.295 We have received a number of stakeholder submissions on the design and effectiveness of remedies relating to product availability and product functionality.

W.296 A number of stakeholders[203] submitted that this remedy should be designed as a combination of specific requirements and principles. For example, CCIA told us that this form of remedy might be most effective with a mix of specific requirements

[203] CCIA response to the Licensing working paper dated 06 June 2024, page 3; Submissions to the CMA [✂].

(to spur immediate action) and principles (to avoid workarounds that undermine the effectiveness of the intervention).[204]

W.297 One cloud provider suggested a non-price remedy could include the use of FRAND-based obligations, with remedy design potentially including guidance as to specific (existing) restrictions which would not be considered FRAND.[205]

W.298 One customer told us that enabling what it referred to as 'platform-agnostic software licensing' across cloud providers could remove licensing as a barrier to multi-platform use, thereby promoting flexibility and reducing vendor lock-in, and that any restrictions on portability should be objectively justifiable.[206]

W.299 AWS provided specific examples of non-pricing restrictions that it considers should be included in remedies relating to Microsoft's licensing practices [✂][208]

W.300 CCIA told us that Microsoft should not be able to mandate how other providers use licences, as this could create operating inefficiencies. CCIA submitted that, as shared hardware is the more efficient way to get things done, you will make competitors less efficient by requiring dedicated hardware.[209]

W.301 Oracle submitted that any remedies around functional parity and equal access could potentially be dealt with through bilateral agreements between Microsoft and cloud providers, to enable the burden on costs to be shared. It said a remedy in which the software provider has all the responsibility and burden is not viable.[210]

W.302 One cloud provider told us that it does not consider that there would be any material costs to Microsoft or third party cloud providers in requiring Microsoft to make software products that are available to run in AWS, GCP and other cloud environments comparable with those that are available to run in Azure.[211]

W.303 Accenture told us that a remedy requiring parity of Microsoft software product and product functionality for use on Azure and non-Azure cloud infrastructure would reduce the technical and pricing advantage of Microsoft Platforms on Microsoft

[204] Note of meeting with CCIA [✂].
[205] [✂] submission to the CMA [✂].
[206] Banking Provider 1's response to the Updated issues statement and working papers dated 23 May 2024 and 06 June 2024.
[207] 'End of life'.
[208] [✂] Note of meeting with [✂].
[209] Note of meeting with CCIA [✂].
[210] Oracle's submission to the CMA [✂].
[211] [✂] submission to the CMA [✂].

Infrastructure, and that the incentive for Microsoft to enable parity is potentially lower as a result.[212]

Microsoft's views:

W.304 Microsoft told us that:

(a) Microsoft's software products work the same across deployments, whether they are deployed on premises on physical hardware, on a VM on premises, or in a cloud on a VM regardless of the cloud provider. Its software runs the same on any supported OS and Microsoft's minimum technical requirements for software are all published and readily available;[213] and

(b) to the extent Microsoft also offers a cloud service, such as SharePoint Online, the cloud service model enables a functionality that the software model does not. Requiring parity of functionality across a cloud service and legacy software would normalise to the lowest common denominator (software model), limiting UK customer access to innovation and improved features.[214]

Design considerations

W.305 In this section we discuss the key design considerations for a product functionality and technical performance remedy, setting out how this remedy could potentially be implemented using the CMA's market investigation powers, while seeking to manage the inherent complexity and circumvention risks of remedies targeted at Microsoft's licensing practices.

W.306 A key design issue for a remedy restricting Microsoft's use of non-price factors is its functional scope. The provisions within this remedy require that customers should have operational equivalence in the use of Microsoft's software regardless of which cloud it is hosted on (ie Microsoft software products should generally perform the same way, and receive the same support, whether they are deployed on Azure or non-Azure clouds).

W.307 We have considered whether the functional scope of this remedy should include more general provisions ensuring parity of user experience on non-Azure clouds. However, based on our evidence and feedback from stakeholders, we considered that these provisions should be included only in specific circumstances. Such

[212] [✂] response to the CMA's information request [✂].
[213] Microsoft's submission to the CMA [✂].
[214] Microsoft's submission to the CMA [✂]. Another cloud provider also submitted that that requiring Microsoft to provide full product equivalence for its software products, regardless of which public cloud they are hosted on, could potentially deter Microsoft from developing new features and harm innovation, or delay the roll-out of new products until such time as they are capable of being rolled out also on non-Azure cloud. [✂] submission to the CMA [✂].

circumstances might include, for example, in relation to interoperability to specific functionality which impacts directly on security.

W.308 Some examples of functionality that we considered could be covered by specific rules-based provisions within the design of this include:

(a) limiting ESUs. These are only available for three years on non-Azure cloud, whereas they are available for four years on Azure; and

(b) the non-availability of certain features for Microsoft's software products that are deployed on other clouds, including in relation to VDI solutions (eg multi-session mode of Windows Desktop).

W.309 In our view, for Microsoft to comply with this remedy would primarily entail making changes to its commercial practices, but might also require Microsoft to make certain technical changes to its software products.

W.310 As identified above, we recognise that, as functional restrictions may impact indirectly on price, there may be overlap between the potential remedies relating to product functionality and technical performance, and pricing. For example, ESUs are free on Azure but need to be paid for when using non-Azure clouds.

Remedy C: Licence transfer

Description of remedy and intended effect

W.311 The third of the inter-related potential remedies that we have focused on would restrict Microsoft's use of licensing practices relating to the deployment of previously purchased software products on a customer's cloud of choice.

W.312 The aim of this potential remedy would be to restrict Microsoft's ability to favour its own cloud services through licensing practices relating to the transfer/deployment of previously purchased software products on the basis of which cloud they are hosted on, which restrict customers' use of the BYOL deployment route depending on their choice of cloud provider.

W.313 We envisage that this potential remedy would comprise:

(a) a principles-based obligation requiring Microsoft not to restrict customers from deploying pre-existing software product licences on the cloud of their choice, other than on a FRAND basis across all cloud providers including Azure;

(b) for those products for which BYOL is currently available, an additional requirement for Microsoft to allow end customers to rely on their on-premises Microsoft software product licences to deploy the Microsoft product on public

cloud, regardless of which cloud it is hosted on, provided they have the necessary licences to do so (eg a relevant subscription license or a perpetual license with active Software Assurance); and

(c) a non-exhaustive list of targeted, rules-based interventions setting out how this principle should be implemented in relation to Microsoft's existing licensing practices.

W.314 We note that any fees charged by Microsoft in relation to the deployment of pre-existing Microsoft software product licences on cloud would need to comply with Remedy A provisions (eg the FRAND pricing requirements).

Stakeholders' views

W.315 Several stakeholders commented on the design and effectiveness of remedies relating to the deployment of pre-existing licences.

W.316 CCIA told us that it considers that licence transfers remedies are central in addressing Microsoft's licensing practices, because this form of remedy has the advantages of both being practical, and being impactful in terms of mitigating barriers to switching. However it also submitted that, as this remedy would not in itself eliminate discriminatory pricing, there should be a mixed remedy approach which also includes prohibitions on discriminatory pricing practices. CCIA commented specifically on the risk of workarounds if Microsoft is able to continue to charge for Software Assurance.[215]

W.317 Oracle told us also that making an offering available and compatible with any cloud without any additional cost is not straight forward and should be considered in detail. It submitted that

(a) a remedy requiring Microsoft to allow customers to deploy software products on non-Azure clouds without any additional cost or charges potentially ignores the benefit to customers from running products on the software provider's platform, and that it is important to recognise the complexities of the work involved in ensuring interoperability; and

(a) it is not clear, for example who is responsible for the costs of ensuring the Microsoft software works on all platforms and also who is responsible for support issues, and that additional cost may also be justified on the basis of additional licence compliance risks that a software vendor runs if its products are deployed on a platform over which it has no control.[216]

[215] CCIA response to Licensing working paper 06 June 2024.
[216] [✂] submission to the CMA [✂].

W.318 In relation to any potential risk of increased unlicensed software use, AWS submitted that any concerns around legitimate customers having more unlicensed use of BYOL on AWS or Google than on other third party cloud services are unfounded.[217] AWS also told us that it is the customer's responsibility to ensure compliance with Microsoft's licensing requirements, that Microsoft already has processes for auditing customers that use its products, and that the tools that AWS provides (eg AWS License Manager) help its customers demonstrate compliance with Microsoft's licensing requirements.[218]

W.319 In relation to the potential risk of Microsoft's incentives to invest in its software products being reduced, one party told us that Microsoft's software products are attractive to customers due to their functionality and widespread use, and a remedy requiring Microsoft to allow customers to BYOL to cloud provider of their choice would not prevent it from monetising its software products, as customers will still need to initially purchase their licence from Microsoft or an appropriate reseller to use it on cloud.[219] This party would expect Microsoft to continue to invest in those products to ensure they stay attractive.[220]

W.320 In relation to the MOU signed between CISPE and Microsoft, [✂].[221]

Microsoft's views

W.321 Microsoft told us that the form of licence transfer remedy set out in our Licensing working paper would fundamentally change Microsoft's UK business model, with adverse consequences all round. Microsoft submitted [✂] and that Microsoft would view that as unjustifiably undermining the core of its existing licensing business model.[222]

W.322 Microsoft further submitted that a remedy which fundamentally altered Microsoft's business model in this way would lead to significant unintended consequences not recognised by the CMA in its Licensing working paper.[223]

W.323 Microsoft told us that a remedy requiring it to extend BYOL rights to Listed Providers would lead to Volume Licensing (VL) options being reduced. Microsoft submitted that [✂].[224]

W.324 Microsoft also told us [✂].[225]

---

[217] AWS' submission to the CMA [✂].
[218] AWS' submission to the CMA [✂].
[219] [✂] submission to the CMA [✂].
[220] [✂] submission to the CMA [✂].
[221] Note of a meeting with [✂].
[222] Microsoft's submission to the CMA [✂].
[223] Microsoft's submission to the CMA [✂].
[224] Microsoft's submission to the CMA [✂].
[225] Microsoft's submission to the CMA [✂].

W.325 Microsoft told us that addressing what Microsoft referred to as 'new mis-licensing challenges' at the scale of AWS and GCP will be hugely complex, costly, and likely not particularly effective.[226]

Design considerations

W.326 In this section we discuss the key design considerations for a licence transfer remedy, setting out how this remedy could potentially be implemented using the CMA's market investigation powers, while seeking to manage the inherent complexity and circumvention risks of remedies targeted at Microsoft's licensing practices.

W.327 The introduction of different pricing and contractual terms for Listed Providers and Non-Listed Providers, as well as the transition to subscription-based licensing, has resulted in different deployment routes and associated pricing structures for Microsoft's software products being available to customers.

W.328 One of the key design considerations for a remedy restricting licence transfers is whether Microsoft should be required to continue offering customers a deployment model which allows them to rely on pre-existing licences when deploying software products for use on cloud.

W.329 We consider that:

(a) for those software products where some or all customers are currently able to rely on their pre-existing licenses for deployment of that product on cloud, Microsoft should be required to extend those rights to all customers on a non-discriminatory basis, regardless of which cloud the software product is hosted on; and

(b) for those software products where this deployment route is not currently available (eg Microsoft 365 Apps), Microsoft should retain the discretion as to whether or not to offer this deployment route, provided it complies with the more general non-discriminatory obligations.

W.330 We recognise that this approach could, in some circumstances, raise distortion risks particularly in the future if Microsoft altered its approach to which future products it extended these rights to, in order to avoid having to offer this on all clouds. However, this could be mitigated by retaining some flexibility within the design and looking to Microsoft's wider conduct (eg in other geographies).

W.331 Another key design consideration was whether Microsoft should be required to allow licence transfer from on-premises to cloud for free, eg in order to address a

[226] Microsoft's submission to the CMA [✂].

potential route for circumvention.[227] However, we consider that the FRAND-based pricing restrictions included in Remedy A would offer a more reasonable approach to managing price-related circumvention risk than an intervention prohibiting Microsoft from monetising licences deployed through BYOL.

W.332 We have also considered how this remedy could be applied in relation to licences purchased as subscription services. We considered that this remedy could require Microsoft to allow customers to transfer licences purchased as subscription services to the cloud of their choice, and that this could apply both to the transfer of subscription services from on-premises to cloud and the transfer of subscription service from one cloud provider to another.[228]

W.333 Finally, we have considered whether this remedy could include rules-based provisions relating to the auditing of unlicensed use of Microsoft's software products. We understand that this is one of the tools Microsoft uses to combat unlicenced use of its products but we also recognise that there is a risk that these processes could potentially be used by Microsoft to preference its own cloud services, for example through gaining access to commercially sensitive information, or making audits overly frequent or burdensome. Therefore, we considered that any remedy design should include provisions relating to Microsoft's audit processes, for example to govern access to, and use of, commercially sensitive information, and ensure that audits are not used in an overly burdensome manner.[229]

Package of remedies and our views on its effectiveness

W.334 We considered that an effective and comprehensive remedy to the AEC that we have provisionally found arising from Microsoft licensing practices would need to comprise a package of principles and rules-based remedies, such as:

Remedy A: Fair, reasonable and non-discriminatory pricing

(a) a high-level principle requiring Microsoft to apply a FRAND approach in relation to pricing its software products, regardless of which cloud they are hosted on;

(b) a non-exhaustive list of targeted, rules-based interventions setting out how this principle should be implemented in relation to Microsoft's existing licensing practices; and

[227] A concern could arise if Microsoft continued to offer these licence transfers, in compliance with the specific requirements of the remedy, but sought to circumvent its effects by raising the associated price to an excessive level such that no customer would choose to do so in practice.
[228] For example, this remedy would require Microsoft to allow customers to BYOL M365 apps to the cloud provider of their choice for deployment on VDIs.
[229] See Chapter 6 on feedback from Microsoft that it does not use this information to preference its own business.

(c) information transparency obligations, requiring Microsoft to publish clear and transparent information relating to the FRAND-based pricing of its software products across Azure and non-Azure clouds.

Remedy B: Product functionality and technical performance

(a) Principles-based obligations requiring Microsoft:

(i) to facilitate a consistent experience for customers who use Microsoft software products on Azure or non-Azure clouds, including in relation to product functionality, unless objectively justified;

(ii) not to take measures which degrade the technical performance of a software product when deployed on non-Azure cloud relative to Azure, for example by withholding access to product functionality; and

(b) a non-exhaustive list of targeted, rules-based interventions setting out how this principle should be implemented in relation to Microsoft's existing licensing practices.

Remedy C: Licence transfer

(a) a principles-based obligation requiring Microsoft not to restrict customers from deploying pre-existing software product licences on the cloud of their choice, other than on a FRAND basis across all cloud providers including Azure;

(b) for those products for which BYOL is currently available, an additional requirement for Microsoft to allow end customers to rely on their on-premises Microsoft software product licences to deploy the Microsoft product on public cloud, regardless of which cloud it is hosted on, provided they have the necessary licences to do so (eg a relevant subscription license or a perpetual license with active Software Assurance); and

(c) a non-exhaustive list of targeted, rules-based interventions setting out how this principle should be implemented in relation to Microsoft's existing licensing practices.

W.335 Any fees charged by Microsoft in relation to the deployment of pre-existing Microsoft software product licences on cloud would need to comply with Remedy A provisions (eg the FRAND pricing requirements).

W.336 In this section we set out our assessment of the effectiveness of the above potential remedies package by examining:

(a) the expected impact on the AEC we have provisionally found and risk profile;

(b) implementation, monitoring compliance and enforcement; and

(c) timescales.

W.337 We then set out our views on the effectiveness of the potential remedies package.

Expected impact on AEC and risk profile

Approach to specification, circumvention and distortion risk in the design of the potential package

W.338 In considering the design of the potential remedies package, we have sought to identify, to the extent possible, ways to minimise the associated risks. Some of the key remedy design choices, aimed at minimising these risks are set out below.

W.339 First, we considered that the potential remedies package could be designed to be implemented as a package of complementary and inter-related remedies targeted at different elements of Microsoft's licensing practices. As set out in Chapter 6, we have provisionally found there are a variety of means by which Microsoft is able to preference its software products, and we considered that a remedy targeted only at some of those practices would be capable of being circumvented.[230] For example:

(a) Microsoft could have the incentive to circumvent Remedy A by restricting the functionality of its software products when deployed on rivals' clouds, unless Remedy A is accompanied by remedies that are targeted at functionality and technical performance of its Software products;

(b) Microsoft could have the incentive to circumvent Remedy B through pricing structures which raise the cost of deploying Microsoft's Software products on a rival's cloud compared with on Azure, unless Remedy B is accompanied by remedies relating to the pricing of those software products; and

(c) Microsoft could have the incentive to circumvent Remedy C by increasing the pricing and fee structures associated with BYOL licence transfer, for example through higher Software Assurance charges, or by degrading the quality of its software products when deployed on a rival's cloud, unless Remedy C is accompanied by remedies targeted also at its pricing practices.

W.340 Second, we considered that an effective remedy should include a combination of principles-based and rules-based measures to manage the specification, circumvention and distortion risks. We are concerned that Microsoft may be able

[230] As part of this assessment, we also considered whether all three of the potential remedies were necessary, or if a subset might be sufficient. In particular, we considered the need to impose restrictions relating to the routes by which Microsoft licenses its Software products (ie Remedy B), or whether these practices could be addressed by instead using Remedy A and Remedy C in combination. However, our view is that this would insufficiently address circumvention risk.

to circumvent a remedy implemented only through rules-based measures, while a remedy designed only as a set of principles would be subject to specification risk, such that it may not be capable of effective monitoring and enforcement.

W.341 Third, to manage the concern that Microsoft, as a vertically integrated firm, could be incentivised to implement a pricing remedy in a way which favours its own business compared with rival cloud providers, this package of remedies would need to require that Microsoft complies with Remedy A through pricing structures that are fair and reasonable, as well as non-discriminatory.

Residual specification, circumvention and distortion risks

W.342 Although we have considered ways in which the design of the potential remedies package could minimise the design and implementation risks, we recognise that the potential remedies package is complex, and that residual risks would remain.

W.343 In particular, our guidance states that to avoid or reduce circumvention risks, behavioural measures will generally need to deal with all the likely substantial forms in which enhanced market power may be applied. In some cases this may not be feasible or may make the behavioural measures complex to monitor and/or enforce.[231] We note that circumvention risks are particularly acute in these circumstances owing to Microsoft having significant market power. This is because, when implementing measures limiting the behaviour of firms with significant market power that has been found to prevent, distort or restrict competition, as is the case here, firms with significant market power may readily evolve new forms of behaviour to replace prohibited or restricted conduct.[232]

W.344 We considered that even after dealing with the circumvention risks that could be addressed through remedy design and through the combination of the three potential remedies into a package, there are still residual risks that this package of remedies could be circumvented through mechanisms such as the introduction of new contractual and pricing structures or monetisation routes, or through technological changes such as updates to Microsoft's software products. For example, Microsoft could seek to alter the way it licences its IP to better reflect a new and emerging business model such that it reintroduces, through a different mechanism, the same effects as those we have provisionally found as contributing to an AEC.

W.345 As noted in our guidance, markets that are subject to frequent change in products or supply arrangements may be particularly prone to specification risk if the definition of required conduct is vulnerable to such changes.[233]

---

[231] CC3 (Revised), Annex B, paragraph 40.
[232] CC3 (Revised), Annex B, paragraph 53.
[233] CC3 (Revised), Annex B, paragraph 40.

W.346 In these circumstances in particular, reflecting Microsoft's position of market power, the nature of the conduct, and connections to wider elements of Microsoft's business, we consider that it would be impractical to predict all possible future variations of the harmful practices that we have provisionally found to contribute to an AEC, and it would be challenging to design rules and principles using the CMA's market investigation powers to adequately address these variations.

W.347 We consider that absent the ability to iteratively adjust the principles-based provisions or to iteratively issue new rules-based ones in a frequent manner, there remains a substantial level of risk that the potential remedies package could be circumvented if implemented using the CMA's market investigation powers.

W.348 Furthermore, due to the complexity of the remedies any initial design would likely require refinement, recalibration and/or correction, particularly over time, in order for the remedies package to provide a comprehensive solution to the AEC we have provisionally found.

Implementation, monitoring, compliance and enforcement

W.349 Even clearly specified remedies may be subject to significant risks of ineffective monitoring and enforcement. This may be due to a variety of causes such as the volume and complexity of information required to monitor compliance, limitations in monitoring resources, asymmetry of information between the monitoring agency and the business concerned and the long timescale of enforcement relative to a rapidly moving market.[234]

W.350 To ensure that a remedy or package of remedies can provide a comprehensive solution to the AEC we have provisionally found, it is important that there are effective and adequately resourced arrangements in place for monitoring and enforcement so that there is a powerful threat that non-compliance will be detected and that action will be taken to enforce compliance where this is necessary.[235] Our guidance states that the effectiveness of any remedy may be reduced if elaborate monitoring and compliance programmes are required.[236]

W.351 We considered that these potential remedies would require significant ongoing monitoring and enforcement, potentially including some form of dispute resolution mechanism.

W.352 We considered that there would be a need for an independent monitoring trustee and/or oversight and implementation entity that had appropriate dedicated

[234] CC3 (Revised), Annex B, paragraph 40.
[235] CC3 (Revised), Annex B, paragraph 41.
[236] CC3 (Revised), paragraph 336 and CMA3, paragraph 4.17.

resources to robustly perform these roles. There would also be a significant ongoing role for the CMA in ensuring compliance monitoring and enforcement.

W.353 Given the inherently technical nature of Remedy B, technical expertise may also be required. For example, we considered that compliance with product functionality obligations would likely need to be independently monitored by reference to a non-exhaustive list of specific functionality requirements, and that such a list would need to be periodically updated, for example in response to product version updates.

W.354 Based on the above, we consider that robustly monitoring and enforcing these potential remedies would likely to be challenging using the market investigation powers, particularly where it is relying on principles-based approaches. This is because the determination of compliance with a principle is, by its nature, less well specified than a narrower rule, and so would be more likely to require detailed ongoing monitoring.

W.355 We considered whether the CMA could establish a body that would perform this oversight and implementation role but we identified certain implementation difficulties associated with this, including:[237]

(a) the need for clarity over the scope, purpose, status and funding of the entity; and the adequacy of its proposed governance arrangements, including periodic future reviews of the effectiveness of the entity's Board and governance;

(a) a clear delineation of the roles, responsibilities and accountability of different stakeholder groups, including the CMA and overall decision-making processes governing each of them;

(b) a process for managing conflicts of interest that may arise within the entity or involving any trustee;

(c) clear lines of communication between the entity, the CMA and external stakeholders;

(d) processes for escalation of issues to the CMA; and

(e) appropriate line management/reporting lines from the external body or any Trustee involved in the implementation process to the CMA.

W.356 We considered that, in principle, such challenges could be addressed in relation to remedies implemented through a market investigation order in many cases. However, we considered that in practice, the monitoring and enforcement

[237] See, for example, Recommendation 4 of the Open Banking Lessons Learned Review that included key factors to consider where a remedy establishes a new entity or large and enduring CMA function.

requirements described above would likely result in the creation of a regime akin to the digital markets competition regime in the DMCC Act. If the CMA were then to designate Microsoft with SMS in cloud services, this could result in overlapping monitoring and enforcement regimes which could raise challenges in terms of regulatory coherence.

Timescales

W.357 We do not expect the AEC we have provisionally found to be time-limited, even if some particular aspects were to change over time (eg licence transfers may become less important if the number of on-premises licences decrease as a result of Microsoft continuing its transition to a subscription-based licensing model for public cloud). Therefore, in the absence of evidence that the harm from Microsoft's licensing practices would reduce over time, we consider that a potential remedies package would need to be for an indefinite duration, albeit with an option to review for changes in certain circumstances.

W.358 As discussed above, many of the specific requirements are likely to need to adapt to changes in the markets and therefore be iterated over time. For example, the cost to Microsoft of providing its individual software products is unlikely to remain fixed, and any changes could have implications for the FRAND price level. These changes are more likely to be necessary over a longer time period.

Our views on remedies to Microsoft's licensing practices that could be implemented through a market investigation order

W.359 As discussed above, we have considered whether the AEC that we have provisionally found in relation to Microsoft's licensing practices is capable of being remedied using the market investigation powers by implementing a package of licensing remedies that includes, in some form, the three measures we have identified as being necessary.

W.360 We have identified risks with implementing this package of remedies using our remedy-making powers under the Act:

(a) impact and risk profile: factors such as Microsoft's position of significant market power, the nature of the practices, the potential for change in Microsoft's software products or supply arrangements, and connections to wider elements of Microsoft's business mean that it would be challenging to address the potential for circumvention without the ability to iteratively develop these measures.

(b) effects of complexity: due to the complexity of the remedies, any initial design would likely require refinement, recalibration, or correction, particularly over time.

(c) monitoring and enforcement: we would expect that this package of remedies would involve an elaborate monitoring and compliance programme, which would involve establishing and maintaining a framework akin to the role envisaged for the CMA under the digital markets competition regime and introduce potentially overlapping regulatory regimes in relation to cloud services.

(d) timescales: long timescales increase the likelihood of circumvention and distortion, particularly as a result of overriding market signals for an extended period. The lack of flexibility to adapt and iterate the remedies package over time increases this concern.

W.361 In principle, it might be possible to address some of these risks in the design of a market investigation order. For example, we have discussed (and dismissed) the potential for establishing a new implementation and oversight body. Alternatively, a market investigation order could seek to introduce greater flexibility through explicit review points for the specific remedy design (eg taking place on a regular time period or being triggered by particular events) to try and ensure that the remedies were effective on an ongoing basis. However, it is not clear that this would allow for sufficient flexibility to comprehensively address the AEC we have provisionally found.

W.362 We consider that if the CMA were to designate Microsoft with SMS in respect of cloud services and consider the imposition of appropriate interventions such as those considered in this report, it would have the ability to iterate remedies over time, as well as have robust monitoring and enforcement powers, which we consider would likely address many (if not all) of the major risks we have identified in our assessment.

Other potential remedies

W.363 The other option that we described in our issues statement to address the AEC we have provisionally found was to prohibit the sale of cloud services as part of a larger bundle that includes cloud services and software.[238]

W.364 As this proposed remedy does not directly relate to the particular licensing practices which we have provisionally found to contribute to the AEC, we do not consider that it would be effective in addressing the AEC we have provisionally found.

[238] Issues statement, paragraph 54.