PART 1: ABOUT CLOUD SERVICES

Cloud computing is the on-demand delivery of compute power, database, storage, applications, and other IT resources via the internet with pay-as-you-go pricing. Thousands of financial institutions, market operators, market participants, and market regulators today use cloud services to run applications and support business critical operations. Cloud services are increasingly being used in financial and securities markets because they provide rapid access to flexible, highly scalable, and low cost IT resources engineered and designed to the highest possible security specifications.

The ability to access and utilise cloud infrastructure and technologies is revolutionising both the delivery of financial services and the supervision of transactions. Using cloud services, market participants are able to respond to market conditions, innovate in an agile manner and increase availability of their services. Independent market regulators like the Financial Industry Regulatory Authority ("FINRA") in the United States can conduct their market supervisory responsibilities with efficacy, efficiency and timeliness. FINRA utilised cloud services provided by AWS to create a flexible platform that adapts to changing market dynamics whilst providing analysts with the tools to interactively query multiple-petabyte data sets.

Regulatory actions targeted at, or applicable to, technology, like the proposed market integrity rules (the "**Proposed Rules**"), need to be drafted using language that encompasses the contractual frameworks used by cloud service providers and their clients. Additionally, it would be beneficial to all Operators and Participants if the obligations created by the Proposed Rules were harmonised with the obligations imposed in similar circumstances by other regulatory bodies. To that end, we note the extensive requirements imposed on regulated financial institutions by the Australian Prudential Regulatory Authority ("APRA") in respect of outsourcing arrangements. These requirements and the way they are articulated are sympathetic to the contractual environment used by cloud service providers.

About AWS

AWS offers 165 fully featured services for compute, storage, databases, networking, analytics, machine learning and artificial intelligence (AI), Internet of Things (IoT), mobile, security, hybrid, virtual and augmented reality, media, and application development, deployment, and management.

These are available from 69 Availability Zones (AZs) within 22 geographic regions and one Local Region around the world, spanning the U.S., Australia, Brazil, Canada, China, France, Germany, India, Ireland, Japan, Korea, Singapore, and the UK. AWS is trusted by millions of active customers around the world – including the fastest-growing start-ups, largest enterprises, and leading government agencies – to securely and reliably power their businesses, make them more agile and lower costs.

PART 2: SUMMARY POSITION

The Proposed Rules will apply to market operators and market participants that outsource critical system functions to third party service providers ("**Service Provider**"), including cloud service providers.

As aforementioned, we believe the Proposed Rules reflect traditional outsourcing concepts that are inherently different to those that apply in relation to the acquisition of cloud computing services. For example, the Proposed Rules appear to assume that the Service Provider: (1) offers a one-to-one, rather than a one-to-many, outsourcing service model; and (2) provides services according to a customer's mandate, as opposed to the customer using services themselves in a self-service environment.

As a result, the Proposed Rules would impose contractual obligations on cloud service providers that they will be unable to fulfil. This will directly restrict the ability of market operators and market participants to adopt, and benefit from the adoption of, cloud services. We do not believe this is ASIC's intent. We have included recommendations below for ASIC's review to address these concerns which are informed by the Australian Prudential Regulation Authority's ("**APRA**") Prudential Standard CPS 231 on Outsourcing[1] ("**CPS 231**).

PART 3: AWS'S DETAILED COMMENTS ON THE PROPOSED RULES – OUTSOURCING OF CRITICAL SYSTEMS

3.1 Chapter 8A, Part 8A.3.3, Paragraph (1)(b)(ii) & Chapter 8B, Part 8B.2.3, Paragraph 1(b)(ii)

Proposed Rules: These Proposed Rules state that an Outsourcing Arrangement contract requires a Service Provider to first obtain the Operator's or Participant's approval prior to: (1) entering into an arrangement with a material subcontractor; and (2) making any material change to the services covered by the Outsourcing Arrangement.

Concern: These Proposed Rules assume that the Service Provider offers a one-to-one, rather than one-to-many, outsourcing service model. Cloud service providers generally offer the same services to all of their customers and therefore are unable to operationalise the requirement to first obtain a customer's approval prior to changing a service, or selecting a material subcontractor. Consequently, mandating cloud service providers to first obtain an Operator's or Participant's prior approval is not appropriate and would directly impact the ability of that cloud service provider to adequately serve their customers across the globe.

Recommendation: We recommend amendments to these Proposed Rules to reflect the language of CPS 231 paragraphs 28 and 29. These paragraphs require an outsourcing arrangement contract to address certain matters but are not prescriptive on how the contract should address them.

[1] https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-231-Outsourcing-%28July-2017%29.pdf

3.2 Chapter 8A, Part 8A.3.3, Paragraph(1)(b)(iv) & Chapter 8B, Part 8B.2.3, Paragraph (1)(b)(iv)

Proposed Rules: These Proposed Rules state that an Outsourcing Arrangement contract must provide for the orderly transfer of services to the Operator or Participant (or another Service Provider) in the event of a termination of the Outsourcing Arrangement contract.

Concern: These Proposed Rules assume that the Service Provider offers services according to a customer's mandate, as opposed to the customer using services themselves in a self-service environment. Cloud services are generally available to customers on a self-service basis without direct assistance from the cloud service provider (including termination assistance services). For example, customers do not need a cloud service provider's assistance to retrieve their content and migrate off the cloud service.

Recommendation: We recommend amendments to these Proposed Rules to reflect the language of CPS 231 paragraphs 28 and 29. These paragraphs require that an outsourcing arrangement contract address certain matters but are not prescriptive on how the contract should address them.

3.3 Chapter 8A, Part 8A.3.3, Paragraph(1)(e) & Chapter 8B, Part 8B.2.3, Paragraph (1)(e)

Proposed Rules: These Proposed Rules state that an Operator or Participant have in place adequate arrangements with their Service Provider to ensure the resilience, reliability, integrity and security of Critical Systems, to maintain the confidentiality, integrity, security, and availability of access to data stored in those Critical Systems.

Concern: Cloud service providers deliver to Operators and Participants the technology infrastructure required to build and deploy technology systems, and to store and process content. The systems built and operated by Operators and Participants on the infrastructure of a cloud service provider remain at all times the responsibility of the Operator or Participant. The Outsourcing Arrangement contract defines responsibilities as between Operators and Participants and their cloud service provider. Unlike traditional outsourcing arrangements, security and compliance responsibilities are shared in cloud services contracts. The responsibilities of an Operator or Participant will depend on the nature of the cloud service and the extent to which the Operator or Participant must perform configuration work or management tasks.

Recommendation: We recommend amendments to the Proposed Rules to reflect the circumstances of cloud Outsourcing Arrangements which involve a sharing of responsibility for the delivery of Critical Systems. This can be achieved by adopting the approach of APRA in CPS 231 that requires outsourcing contracts to address, at a minimum, a range of matters pertinent to the maintenance and operation of Critical Systems. Operators and Participants should also have the means to verify the ability of their cloud Service Providers to fulfil their contractual obligations. To achieve this outcome, we further recommend that ASIC require Operators and Participants to seek access to cloud Service Providers Systems and Organisation Controls ("**SOC**") 1 and 2 audit reports to gain assurance of their security and privacy practices.

3.4 Chapter 8A, Part 8A.3.3, Paragraphs(1)(f)-(g) & Chapter 8B, Part 8B.2.3, Paragraphs (1)(f)-(g)

Proposed Rules: These Proposed Rules state that an Outsourcing Arrangement must ensure the Operator or Participant (and their auditors) have prompt access, on request, to books, records, and other information of the Service Provider relating to the Critical Systems. Additionally, an Outsourcing Arrangement must also ensure that ASIC has the same access to these books, records, and information.

Concern: The scope of requested information is very broad. For example, these Proposed Rules might require a cloud service provider to provide critically sensitive information about its infrastructure, security or services. Such information may include highly sensitive and secret details of the Service Provider's operational security environment. The loss or unauthorised disclosure of this information would put the cloud service provider and its customers at significant risk and could have implications for global security certifications held by the cloud service provider. Additionally, because cloud services are generally self-service by nature, the cloud services customer, and not the cloud services provider, will control its own systems architecture and data governance rules relating to the Critical Systems.

Recommendation: We recommend amendments to these Proposed Rules to reflect the language of CPS 231 paragraph 34. Specifically:

(a) the Outsourcing Arrangement contract must include a clause allowing ASIC to access documentation and information related to the Outsourcing Arrangement (defined as relevant information and documentation regarding the technical and organisational measures of the cloud service provider and its affiliates and about the Outsourcing Arrangement contract); and

(b) Where possible, ASIC will, in the first instance, seek to obtain the information it requires from the Operator or Participant.