Microsoft Submission in response to the proposed Financial Market Infrastructures Standards Consultation

Submission to the consultation process run by the Reserve Bank of New Zealand and Financial Markets Authority.

November 2022

1. Introduction

1.1. Microsoft welcomes the opportunity to present this submission to the Reserve Bank of New Zealand – Te Pūtea Matua, and the Financial Markets Authority – Te Mana Tātai Hokohoko (together, the **Regulators**) in response to the FMI Standards Exposure Drafts. This submission builds on our previous work the with Reserve Bank of New Zealand on its Cyber Resilience Draft Guidance, and we hope it provides further perspective on the role of Microsoft's cloud solutions in FMI operations.

1.2. Our submission focuses on FMI Standard 17B: Critical Service Providers (**Draft Standard**) and the associated draft guidance (**Draft Guidance**). Microsoft is broadly supportive of the Draft Standard, and recognises the importance of ensuring Financial Market Infrastructure (**FMI**) operators have robust risk mitigation practices in place with Critical Service Providers (**CSPs**).

Our involvement in FMIs

1.3. Microsoft is a major provider of cloud services, software and other technology solutions to FMI operators. As such, we may be classified as a CSP under the Draft Standard. We understand the importance of maintaining the stability and security of New Zealand's financial system, as well as our role in supporting the operational resilience of our FMI operator and CSP customers.

1.4. We are an industry leader in cloud computing security and resilience. Among other certifications, our cloud services are compliant with ISO/IEC standards on Information Security Management and Protection of Personal Information, a rigorous set of global standards for physical, logical, process and management controls used in cloud computing. A full list of our compliance offerings is available on our website.[1] Our internal technical and organisational systems are also designed to meet the risk assurance requirements of global financial institutions, and we make a number of related commitments in our Online Services Terms.[2]

1.5. If the Regulators would benefit from further background on the use of our cloud computing in the financial services sector, our response to the Australian Prudential Regulation Authority's (**APRA**) Information Paper on Cloud may be helpful. [3] Although APRA operates in a different regulatory environment, our response addresses the potential risks of cloud computing in the financial sector, and provides additional detail on our cloud services more generally.

---

[1] microsoft.com/en-us/trustcenter/compliance/complianceofferings

[2] https://www.microsoft.com/en-sg/Licensing/product-licensing/products.aspx

[3] Microsoft, Microsoft's response to APRA's 2018 Information Paper on Cloud, RE2GKgS (microsoft.com)

Overview of our submission

1.6. It appears to us that many of the requirements in the Draft Standard and Draft Guidance may be aimed at CSPs providing financial and operational services to FMIs, for example, custodial services, sub-clearing services or market administration services. These services are usually tailored to at least some degree to accommodate the specific characteristics of the FMI they support.

1.7. By contrast, the services we provide to FMIs are generally highly standardised, 'hyperscale' solutions, supplied to a global customer base spanning many industries and sectors. Our Microsoft Azure cloud offering is a good example. Microsoft Azure is a platform upon which our customers and their third party service providers can build solutions tailored to their own needs, but the platform itself is wholly standardised and consumed in a utility-like manner.

1.8. There are two broad models for how 'hyperscale' cloud platforms might be incorporated as part of a critical service relied on by an FMI operator. In a 'bundled' model, a platform subscription is purchased and paid for by the CSP, which then builds its own services on top of the platform and provides a bundled solution to the FMI operator. In an 'unbundled' model, the platform subscription is purchased and paid for by the FMI operator, which then engages its own third party service providers to build and deploy applications and services on top of the platform. The most appropriate model varies between different applications and services.

1.9. As we outline in more detail below, some aspects of the Draft Standards and Draft Guidance may not be appropriate for all CSP types, and in particular, may make it more difficult than necessary for FMI operators to make use of the 'unbundled' delivery model, even in cases where it may provide benefits for the FMI operator's resilience and risk management.

1.10. Accordingly, our submission makes the following recommendations:

a) The 'reasonable steps' required of FMI operators should expressly allow for risk mitigation options available to the FMI operator *outside* of the relationship with any one CSP.

b) Where the CSP is providing a highly standardised technology service, the FMI operator should not be required to impose requirements on the CSP relating to general "enterprise risk management", as distinct from risk management for business continuity and information security.

c) Where the CSP is providing a highly standardised technology service, any technology lifecycle planning obligations would be more appropriately placed on the FMI operator.

2. Allowing a flexible approach to risk mitigation

2.1. Elements of the Draft Standard and Draft Guidance may be more prescriptive than necessary, insofar as they could be read as requiring FMI operators to obtain the same type of assurance in each and every CSP arrangement, regardless of the nature of the CSP or the criticality of the service they provide to the FMI. Similarly, clause 2(a) of the Draft Standard reads as if it imposes 'strict' obligations, which may unnecessarily constrain the methods available to the FMI operator to achieve the objectives of the clause.

2.2. Clause 1 of the Draft Standard requires FMI operators to take all reasonable steps to "ensure the continued provision of critical services by managing the relationship with its critical service providers". It is not clear from this wording whether an FMI operator can accept a lower level of continuity assurance for one CSP if the risk is mitigated by other contingency arrangements available outside its relationship with that individual CSP.

2.3. There may be situations where the best risk mitigation strategy is a mix of services from several CSPs providing a degree of redundancy, rather than 'gold plated' continuity arrangements with each individual CSP. We think it would be desirable to clarify that the "reasonable steps"

required of FMI operators could also encompass these alternative risk mitigation strategies. This is especially relevant in the context of a 'hyperscale' cloud platform, where there may be limits on the extent to which the platform provider can accommodate bespoke requirements for the FMI operator, but it may be possible to mitigate the residual risk outside the relationship with that individual CSP.

2.4. Further, clause 2 of the Draft Standard states that:

> *2) Further to the requirements in clause (1), an operator must take reasonable steps to ensure that a FMI's critical service provider:*
>
> *a) identifies and manages relevant operational and financial risks to the provider's ability to provide critical services to the FMI,* ***this includes ensuring that****:*
>
> *i) the provider implements and maintains appropriate policies and procedures for the continued provision of critical services;*
>
> *ii) the provider has effective risk management processes;*
>
> *iii) the provider's critical services are available, reliable, and resilient; and*
>
> *iv) the provider has robust business continuity management plans and disaster recovery plans to support the timely resumption of its critical services in the event of an outage so that the provider fulfils the terms of its agreement with the operator or FMI, as appropriate;*

2.5. The wording highlighted above in bold reads as if the FMI operator has a *strict* obligation to ensure that the requirements of sub-paragraphs (i) through (iv) are met. This may lead FMI operators to assume that these requirements need to be flowed down to CSPs as strict contractual obligations, especially in light of paragraph 17B.2 of the Draft Guidance.

2.6. This may prove difficult for FMI operators when dealing with CSPs that are 'hyperscale' platform providers, as there will be limits on the extent to which such CSPs are able to contractually 'guarantee' those outcomes. Consistent with the more general overall standard required by clause 2, it would be desirable to clarify that clause 2(a) likewise requires only *reasonable steps* from the FMI operator, which are bound to vary depending on the context.

Recommendations

2.7. We recommend updating the Draft Guidance to include statements to the effect that, in determining what is required by way of "reasonable steps" under the Draft Standard, the FMI operator should take into account the criticality of the services to the operation of the FMI, including any contingency arrangements that the FMI operator may implement outside its relationship with a particular CSP, in order to mitigate the risks of a failure by that CSP.

2.8. We recommend amending clause 2 of the Draft Standard as follows:

> *2) Further to the requirements in clause (1), an operator must take reasonable steps to ensure that a FMI's critical service provider:*
>
> *a) identifies and manages relevant operational and financial risks to the provider's ability to provide critical services to the FMI, this includes taking reasonable steps to ensure: […]*

3. Requirements for enterprise risk management

3.1. The Draft Standard and Draft Guidance require FMI operators to obtain assurance from CSPs in relation to their risk management practices. These obligations may not be appropriate in the context of 'hyperscale' platform offerings.

a) Clause 2(a) of the Draft Standard requires FMI operators to take reasonable steps to ensure each of their CSPs:

… identifies and manages relevant operational and financial risks to the [CSP's] ability to provide critical services to the FMI…

b) Paragraph 17B.5 of the Draft Guidance states:

An operator should take reasonable steps to ensure that a critical service provider has effective processes and systems for:

a) identifying and documenting risks;

b) implementing controls to manage risks; and

c) making decisions to accept certain risks.

c) Paragraph 17B.7 of the Draft Guidance requires that:

An operator should take reasonable steps to ensure that the identification and management of risks is being overseen by the critical service provider's board of directors and assessed by an independent, internal audit function.

d) Paragraph 17B.2 of the Draft Guidance elaborates on the Regulators' expectation that these requirements (among others):

… would be met through the terms of a contract between the critical service provider and an operator wherever possible. However, there may be circumstances where this is not reasonable, such as where there is no existing contract between an operator and the critical service provider, or because it may take several years for a contract to be negotiated.

3.2. Microsoft supports the principles in clause 2(a) of the Draft Standard, and paragraphs 17B.5 and 17B.7 of the Draft Guidance, but submits that paragraph 17B.2 of the Draft Guidance may be too prescriptive in its present form when considered against the current practices of major technology providers.

3.3. It is common for major technology providers to give robust contractual commitments in relation to managing data security and business continuity risks, but this is not the case for enterprise risk management more generally. Accordingly, paragraph 17B.2 of the Draft Guidance may put FMI operators in a difficult position, if it requires them to obtain from their technology CSPs contractual commitments that CSPs are not able to give.

3.4. Similarly, due to commercial sensitivity and legal constraints, it may be difficult for many publicly-traded technology providers to give FMI operators granular information about their enterprise risk management processes and procedures, beyond what has already been disclosed in publicly available documentation.

3.5. If these requirements make it more difficult for FMI operators to adopt 'hyperscale' technology solutions, this may inadvertently nudge FMI operators towards solutions optimised for formal compliance with prescriptive regulatory requirements, rather than solutions that genuinely provide the best combination of performance, cost effectiveness and risk management.

3.6. By way of comparison, it is worth noting that APRA's draft CPS230 standard[4] does not require any "flow down" of enterprise risk management requirements to service providers.

Recommendations

3.7. We recommend supplementing paragraph 17B.2 of the Draft Guidance to reflect that there may be other circumstances in which it is reasonable for an FMI operator to proceed *without* contractual commitments from a CSP regarding its general enterprise risk management practices. For example, if the FMI could satisfy itself via a due diligence exercise, assessing the CSP's track record and/or publicly available information on the CSP's risk management practices.

3.8. We would also recommend updating paragraph 17B.17 to accommodate the fact that it would be unusual for major technology providers to provide customers with granular information about their enterprise risk management processes and controls, as distinct from more targeted information on processes and controls addressing data security and business continuity risks.

4. Technology Lifecycle Planning and communications

4.1. Section 2(c) of the Draft Standard requires the FMI operator to ensure that its CSP:

… has in place robust methods to plan for the entire lifecycle of the use of its technologies and the selection of technological standards;

4.2. The Draft Guidance elaborates on this requirement in paragraph 17B.14:

Proposed changes to a critical service provider's technology should include a comprehensive consultation with an operator and, where relevant, its participants. An operator should require a critical service provider to regularly review its technology plans, including assessments of its technologies and the processes it uses for implementing change.

4.3. FMI operators may find it difficult to procure their technology CSPs to meet or contractually commit to these requirements. Technology lifecycle planning is a core activity for Microsoft – our methods and practices in this area are not only robust but industry-leading. However, as a provider of 'hyperscale' services that support a large global user base, Microsoft does not give contractual commitments to consult on technology changes with individual customers. The same will be true for many other major technology providers.

4.4. We submit that an obligation of this kind is best placed on the FMI operator, rather than requiring FMI operators to impose it on CSPs. It will be the FMI operator that selects what technologies and technological standards it uses to operate the FMI, and plans for how those technologies and standards will be supported and eventually replaced. This in turn will drive the FMI operator's choice of CSPs. The most critical lifecycle planning will be the FMI operator's own selection, engagement and eventual replacement of the CSPs themselves.

4.5. The Draft Standard and Draft Guidance also require CSPs to consult with FMIs and the broader market (i.e. participants) on technical changes to the CSPs operations that could impact its risk profile. Paragraph 17B.17 of the Draft Guidance states:

As a part of its communication procedures and processes, a critical service provider should be expected to have mechanisms to consult with the FMI and the broader market on any technical changes to its operations that may affect its risk profile, including incidences of absent or non-performing risk controls of services.

[4] https://www.apra.gov.au/sites/default/files/2022-07/Draft%20Prudential%20Standard%20CPS%20230%20Operational%20Risk%20Management.pdf

4.6. Such a requirement makes sense for a CSP providing tailored financial or operational services to an FMI operator, but probably not for a CSP providing more generic technology services. As noted above, as a provider of 'hyperscale' services that support a large global user base, Microsoft does not give contractual commitments to consult on technology changes with individual customers. The same will be true for many other major technology providers.

4.7. By way of comparison, it is worth noting that APRA's draft CPS230 standard[5] does not require APRA-regulated entities to impose lifecycle planning or communications requirements on their service providers.

Recommendation

4.8. To address the matters outlined above, we recommend the technology planning requirements in the Draft Standard and Draft Guidance be revised to focus on lifecycle planning by FMI operators rather than by CSPs.

4.9. Alternatively, it may be sufficient to clarify that the technology planning requirements in the Draft Standard and Draft Guidance are not intended to apply to standardised technology services that are not tailored by the CSP specifically for the FMI.

4.10. Finally, we recommend revising paragraph 17B.17 of the Draft Guidance to clarify that FMI operators are not expected to require technology providers to consult on technical or operational changes to standardised 'utility-like' service offerings, as distinct from technology services that have been tailored by the CSP specifically for the FMI.

5. Conclusion

5.1. Microsoft thanks the Regulators for the opportunity to review and provide feedback on the Draft Standard and Draft Guidance. Overall, we see these regulations as being a necessary step in ensuring the reduction of FMIs' operational risk. Microsoft hopes that the challenges and recommendations in our submission are of assistance to the Regulators in the finalisation of the Draft Standard and associated guidance.

5.2. Please do not hesitate to contact our team should you have any questions.

[5] https://www.apra.gov.au/sites/default/files/2022-07/Draft%20Prudential%20Standard%20CPS%20230%20Operational%20Risk%20Management.pdf