Reserve Bank of New Zealand

By email: cyberresilience@rbnz.govt.nz

29 January 2021

MICROSOFT'S RESPONSE TO THE RESERVE BANK OF NEW ZEALAND'S DRAFT GUIDANCE ON CYBER RESILIENCE

Thank you for the opportunity to provide a response to the Reserve Bank of New Zealand's (RBNZ) Draft Guidance on Cyber Resilience (the Draft Guidance).

Microsoft strongly supports the general approach taken by RBNZ in developing the Draft Guidance, including its intention to draw upon international standards and provide principle-based, proportionate guidance to enhance the cyber resilience of New Zealand's financial sector.

This document offers a number of suggested revisions to the Draft Guidance, based on our experience working with financial services institutions and regulators in other jurisdictions.

Background

The evolution of consumer expectations as to the level and types of service provided by banks and other financial service institutions (FSI), as well as financial services market competition, has led to rapid cloud-based innovations in the financial services sector. Microsoft considers itself to be a partner to RBNZ's regulated entities with respect to innovation, cyber security and cyber resilience.

In Microsoft's view, the implementation of cloud-based innovations and the shift to use of cloud computing services does not require any compromise of security. In fact, in many respects, hyperscale cloud services, such as those provided by Microsoft, are fundamentally more secure than on-premises software or private datacentres.

In our experience, New Zealand FSIs may still be unclear as to whether cloud solutions are permitted within the regulatory environment that those FSIs operate under. A conservative non-cloud approach can lead to much higher costs for New Zealand-based FSIs when compared to their international counterparts, fewer opportunities for innovation, and lower levels of security than could be achieved with a cloud-based approach.

Microsoft recognises that RBNZ's role is to promote security and cyber resilience within New Zealand's financial sector as a whole, and not to assess whether particular technologies are more or less suitable to meet security expectations from a business perspective. That said, given the sector's lack of certainty as to whether cloud services meet regulatory expectations, we think RBNZ has a great opportunity to drive clarity, and recognise that FSIs can meet cyber resilience targets while still advancing innovation through cloud-based solutions.

Specific recommendations

1. Microsoft strongly supports RBNZ's approach of aligning the Draft Guidance with international practices and adopting a high-level set of principle-based recommendations. A principle-based, outcome-focused approach, as opposed to a prescriptive set of requirements, will provide FSIs with the necessary ability to adapt as technology evolves. Aligning with international practices will also help manage an unnecessary compliance burden, particularly for FSIs dealing with international service providers already meeting international cyber resilience standards.

2. Microsoft supports the recommended considerations outlined in Part B (Capability Building). Based on our experience with FSI customers, we recommend that it be made clear that this section applies to the FSIs' own systems, and not to outsourced cloud services. With respect to any requirements relating to outsourced cloud services, we recommend that those be set forth (only) in Part D. This is an important clarification as the appropriate and feasible measures will differ in accordance with the shared responsibility model for cloud services. For example:

   B1.3: Where the FSI is using hyperscale public cloud services, it should be made clear that the requirement to map network resources is not applicable to the cloud service provider's (CSP) private network or data centre connections. While it is good practice for customers to document their virtual networks in a CSP's cloud and any VPNs, private and public peering, or dedicated connections to a CSP's cloud, the CSP will control the network resources relating to its service, and it may not be able to provide such detailed information to its customers. FSIs should instead be advised when using hyperscale public cloud services to review audit reports and other information relating to the CSP's network resources.

   B.1.4.1: In the case of updates or new features or services, where such are part of hyperscale public cloud services, the CSP will conduct appropriate testing and assessment of threats or vulnerabilities. The FSI should ensure the CSP does so, but should not be required to itself do so with respect to hyperscale cloud services as it is often impractical or simply not possible. For example, in the SaaS service model the updates simply become part of the standard service offering. In regards to other types of cloud computing services (such as IaaS or PaaS), the customer often has greater discretion as to when it leverages a new feature or service in production.

   B.3.7: An FSI should not be required to conduct penetration tests on a CSP's networks used to provide hyperscale cloud services. Instead, it should be required to confirm that the CSP conducts regular penetration testing.

   B4.7: An FSI should not be required to conduct or participate in an ex post root cause analysis of cybersecurity incidents to the extent they involve hyperscale cloud services as such participation is not possible, and it may not be feasible for an FSI to receive detailed information regarding root cause analyses from a CSP. An FSI should review a CSP's ISO 22301 processes relating to incident response and recovery and, where cybersecurity incidents involve hyperscale cloud services, the FSI should ensure that the CSP conducts adequate root cause analyses of such incidents.

   B4.8.1: It is not feasible (nor is it relevant) for FSIs to jointly test response and recovery plans with CSPs. Where hyperscale cloud services have been deployed, the FSI should ensure that the CSPs regularly test their response and recovery plans (and that the FSI tests its own plans which supplement the CSP plans).

In addition to clarifying how the requirements may differ in the case of hyperscale public cloud services, it would be helpful to specify where any required measures should be included in contract terms or where they are part of a risk assessment, due diligence or compliance exercise (keeping in mind that CSPs may be limited in terms of the specific terms that can be included in evergreen contracts).

3. Microsoft is concerned that the preamble to Part D (Third-Party Management) of the Draft Guidance may present the adoption of cloud services as more of a risk than an opportunity. In Microsoft's experience, there is a high degree of uncertainty amongst regulated entities regarding the use of cloud services and whether it is permitted at a regulatory level. The approach in the preamble may add to FSI's confusion as to whether they are able to implement cloud solutions while complying with their regulatory requirements or maintaining appropriate cyber resilience capability. Microsoft's preference would be for the language in Part D's preamble, particularly the last paragraph, to be more positive while preserving the acknowledgement that FSIs still need to ensure they have adequate safeguards and risk mitigation measures in place. For example, see the Australian Prudential Regulatory Authorities comments in its 2018 Information Paper on the advancement of cloud service offerings.[1]

4. Microsoft notes the reference to concentration risks to the financial system, also in the preamble to Part D of the Draft Guidance. However, the Draft Guidance does not cover how such risks should be addressed by RBNZ's regulated entities. Microsoft recommends that the guidance address how entities could manage concentration and vendor lock-in risks, for example through the development of exit and migration plans, or geographic diversity (by linking the Part D preamble reference to concentration risk to section D8.6). Hyperscale cloud infrastructure is itself very complex with strong resilience measures in place to mitigate against point-of-failure risks that may arise, for example, in a geographical region or a particular data centre.[2]

5. D3.1: It would be helpful to specify which issues should be addressed in the contracts with CSPs. For the reasons noted above, some requirements should not be required to be included in contracts. If overly specific terms are requested to be included, it may, in fact, hinder the CSP's ability to adopt new best practices or to take advantage of technological advancements.

6. D4 1.4: As outlined above, it is not feasible for CSPs, at least those providing hyperscale cloud services, to conduct joint testing with customers. Nor is it necessary, as the CSP's response plan and responsibilities will not overlap with the FSI's. Microsoft recommends that this provision be amended to state: "Ensure third parties that provide services for the entity's critical functions have adequate response plans that are tested regularly."

---

[1] "Since 2015, there has been continuous evolution of both cloud computing service offerings and APRA-regulated entities' risk management. Generally, service providers have strengthened their control environments, increased transparency regarding the nature of the controls in place, and improved their customers' ability to monitor their environments. APRA-regulated entities have also improved their management capability and processes for assessing and overseeing the services provided." APRA Information Paper on Outsourcing involving Cloud Computing Services, September 2018, page 4.

[2] See also the following Microsoft resources addressing exit planning and concentration risks in the financial services industry:

Exit planning whitepaper: http://aka.ms/MicrosoftExitPlan

Concentration risk whitepaper: https://azure.microsoft.com/mediahandler/files/resourcefiles/concentration-risk-perspectives-from-microsoft-/Concentration_Risk_Perspectives_062020.pdf

7. D8.1: Microsoft would like to see clarification included in the guidance regarding the purpose of the recommendation at paragraph D8.1, that regulated entities should "inform RBNZ about their outsourcing of critical functions to CSPs early in their decision-making process". In Microsoft's experience working with regulated entities, without clarification such a recommendation is likely to be interpreted as a tacit requirement to seek *ex ante* approval from the regulator for the use of cloud services. It is Microsoft's understanding that this is not RBNZ's intention.

8. Microsoft is also concerned with the recommendation at paragraph D8.3 that regulated entities should "know... where their data will be stored, processed and transmitted". We understand the need to consider jurisdictional risk for any data storage or data at rest. However, the location of data during transmission (data in transit) and computing/processing (data in use) should not be equalised with the location of stored data. Data in transit and data in use in cloud computing is generally ephemeral and encrypted and so doesn't create the same data location and sovereignty issues (such as law enforcement access rights) as stored data or data at rest.

   By way of example, Microsoft makes commitments to store customer data at rest in certain major geographic areas. Customer data that is transmitted or otherwise processed is not subject to geographical restrictions but instead subject to technical and organizational measures that comply with ISO 27001, ISO 27002, and ISO 27018 to protect such data. Customer data in transit is encrypted by default. Differentiating location commitments for different states of data in this way does not diminish the protection of the data.

RBNZ's cyber resilience guidelines have the potential to provide desired clarity for the financial services institutions operating in New Zealand and increase the overall cyber resilience of New Zealand's the financial services market. Microsoft hopes the above recommendations will help RBNZ in developing the guidance by enhancing the value of the guidelines for FSIs and addressing real-world issues arising in this domain.

Microsoft is committed to protecting all organisations in the cyber world and we can be available to answer any questions you may have regarding this submission and to provide additional input that may be of help in the guidelines' development process or their subsequent practical implementation with the financial institutions.

Kind regards,

Maciej Surowiec
Government Affairs Lead
Microsoft
[redacted]