29 January 2021

Dynamic Policy Team
Financial System Policy and Analysis
Reserve Bank of New Zealand
PO Box 2498
WELLINGTON 6140

Email: cyberresilience@rbnz.govt.nz

RE: CONSULTATION DOCUMENT – RISK MANAGEMENT GUIDANCE ON CYBER RESILIENCE AND VIEWS ON INFORMATION GATHERING AND SHARING

Amazon Web Services (AWS) welcomes the opportunity to make a submission to the Reserve Bank of New Zealand (RBNZ) in respect of the abovementioned consultation document. AWS supports the RBNZ's intention, outlined in its November 2019 Financial Stability Report, to become more proactive in promoting cyber resilience in New Zealand's financial sector. This is an important, and appropriate, step for the RBNZ given the current, and forecast, risks of cyber-attacks on the technology of financial institutions.

AWS has considered the RBNZ's rationale for regulatory intervention and reviewed the draft cyber risk management guidance for regulated industries. Noting the public interest in maintaining confidence in the efficient and effective operation of a resilient financial system, AWS endorses the RBNZ's 'moderately active' policy stance and its identification of three activities to implement that stance: the issuance of risk management guidance; information gathering and sharing arrangements; and enhanced incident response coordination protocols for public and private sector bodies.

AWS acknowledges that each of these elements will require progressive development and an iterative implementation in a rapidly changing technology landscape. AWS appreciates the RBNZ's collaborative intention. In addition to our general comments regarding the approach to cyber resilience outlined by the RBNZ and the questions posed in the Consultation Document, AWS has included comments in this submission on the Draft Guidance; most particularly Part D as it concerns Cloud Service Providers (CSPs).

If possible, we would be delighted to follow up this submission with an opportunity to sit down with your team to discuss these issues further – we have NZ-based experts who would be able to travel to Wellington at a time of your convenience.

Yours sincerely,

Roger Somerville [redacted]
Head of Public Policy, Australia and New Zealand
Amazon Web Services.

GENERAL COMMENTS

In March 2019, AWS released a Whitepaper titled "*Amazon Web Services' Approach to Operational Resilience in the Financial Sector and Beyond*" which described how AWS and its customers in the financial services industry achieved operational resilience using AWS services. The Whitepaper acknowledged that both financial services customers and AWS had a common interest in maintaining operational resilience, defined as the ability to provide continuous service through people, processes, and technology, that are aware of and adaptive to constant change. This interest is also held by the RBNZ as the regulator of financial services in New Zealand.

AWS recognises that continuity of service is a key prerequisite for financial stability. Financial services customers rely on AWS to provide resilient infrastructure and services that enable them to design and operate applications in a manner that meet their regulatory and compliance obligations. Achieving operational resilience requires AWS to be responsible for ensuring that the services used by our customers are continuously available. This necessitates that AWS is able to handle a wide range of events that could affect our infrastructure, including all cyberattacks targeted at our infrastructure.

Our financial services customers must similarly be able to design, deploy, and test their applications on AWS to achieve both the availability and resiliency they need, including for mission critical applications that must operate with almost no downtime.

This dual approach to operational resilience is something we call "shared responsibility". Cloud security is an example of shared responsibility. AWS manages security *of* the cloud by ensuring that AWS infrastructure meets or exceeds global and regional regulatory requirements and best practices, but security *in* the cloud is the responsibility of the customer. Our customers retain control of the security program they choose to implement to protect their own content, platform, applications, systems and networks, no differently than they would for applications in an on-premise data centre.

A copy of the AWS Whitepaper on operational resilience in the financial services sector is attached for your reference.

As noted in the Consultation Document, risk and incident reporting requires a collaborative approach to be successful. Every entity in the financial services ecosystem that contributes to the technology used by financial institutions can contribute to better understanding of systemic cyber threats and risks. AWS notes that incident information sharing is an after the fact exercise. While important and valuable to understanding risk vectors and specific attacks, it should be considered secondary to building confidence through the systemic adoption and reporting of proven approaches to information security.

AWS has obtained certifications and independent third-party attestations for a variety of industry specific workloads. These certifications and attestations include ISO 27001, ISO 27017, ISO 27018, ISO 9001, PCI DSS Level 1, SOC1, SOC2, and SOC 3. Through an on-going global compliance program, and a continuous risk assessment process, AWS aims to identify, evaluate, and mitigate risks across both its physical cloud infrastructure and cloud services, as well as the company more generally. AWS customers can access copies of these independent certifications and attestations. This provides our customers with the assurance that we can and do fulfil our obligations under the shared responsibility model to maintain the operation and security of the AWS cloud.

REPONSE TO CONSULTATION QUESTIONS

Q1: In light of the nature of cyber risk and the range of observed international practices discussed in the previous section, do you support the Reserve Bank's policy stance of being 'moderately active' in promoting cyber resilience within the financial sector?

Innovation in policy, just as in technology services and products, inevitably implies risk. Without innovation however, existing risks cannot be mitigated and opportunities cannot be realised. The RBNZ's proposed policy stance is, in the circumstances of rapid innovation and increasing cyber threats, reasonable and proportionate.

Q2: Do you agree with the Reserve Bank's general approach of sticking closely to international practice? Do you have any specific feedback on the draft guidance on cyber resilience?

We absolutely agree. We welcome the RBNZ's efforts to advance the discussions on cyber resiliency and align their regulatory strategy with international security practices. Given the global nature of both finance and technology, coordination and harmonization across global jurisdictions is critical in order to secure a level playing field and avoid fragmentation.

Please see further down in our submission for specific feedback on the draft guidance on cyber resilience.

Q3: Do you agree that the guidance should be a set of high-level principle-based recommendations?

Given the rapid level of technological innovation, we strongly believe any regulatory initiatives should remain flexible enough to handle increasingly dynamic complexities in the financial and technology spaces. AWS fundamentally believes in the value of globally resonant and actionable financial regulatory principles and laud the RBNZ for taking a less prescriptive and principles-based approach to strengthening cyber resilience which affords financial service entities the flexibility to address cyber resilience in the context of their size, complexity and risk profile.

Q4: What's your view on the principle of proportionality and a risk-based approach adopted by the Guidance?

The RBNZ's adoption of the principle of proportionality throughout the guidance is noted and AWS considers it an appropriate principle to adopt across a commercial sector. AWS notes that the execution of any cybersecurity strategy requires the making of priority value judgments, particularly about levels of resourcing and investment. Consequently, it is appropriate that considerable weight be given in the guidance to the accountability of Boards and Senior Management of regulated entities defining, accepting and executing their duties to assess and respond to risks through strategies to achieve cyber resilience.

Q5: Do you agree that the guidance should apply to all regulated entities of the Reserve Bank?

In line with ensuring public confidence in, and the resilience of, the financial system, AWS agrees the guidance should apply to all regulated entities of the RBNZ.

Q6: What's your view on the Reserve Bank's collaborative and coordinated approach to information gathering and sharing?

To be successful, reporting arrangements need to be proportional, pragmatic, and result in improved cybersecurity outcomes. Proportional in this context refers not only to the cost of collection but to the value the collected information provides to greater resilience across the sector. Pragmatic requires that the volume and level of information collected not only contributes to better generic cybersecurity outcomes but is capable of being collected in a manner that is feasible for all relevant entities.

The outcome of collecting information should not merely be statistical. There should be clear processes and systems within those entities that collect information for using the information to produce better security outcomes overall as measured by increased system resilience. A data collection system should be connected to a reliable and transparent operational process.

Confidence in the protection of highly sensitive collected information is vital – as is acknowledged in the Consultation Document. The creation of an information 'honeypot' should be expressly avoided through data collection minimisation policies and the application of the highest levels of data security and access privilege rules to all the collected information.

Q7: Do you support the Reserve Bank's intention to broadly follow the international practices and establish a cyber data collection for all prudentially regulated entities? Do you have any particular concerns or issues that you would like the Reserve Bank to take into account when further developing its plan?

AWS supports the adoption of a materiality threshold for reporting cyber incidents and the adoption of a definition of a cyber-incident that focuses on a systemic threat to an entity's information security. AWS also supports the reporting of incidents by

regulated entities promptly after it is possible for such a report to be reasonably made. Reporting times should allow the regulated entity to assess the incident, establish the scope of risk inherent in the incident, and identify if the incident involved an actual or attempt of compromise of data.

Given the increasing use of third party technology providers by entities regulated by the RBNZ, the RBNZ should consider emerging international practices for establishing information sharing arrangements with third party providers. Contractual arrangements between regulated entities and their technology providers will in the first instance establish information sharing protocols in respect of cyber incidents.

DRAFT GUIDANCE ON CYBER RESILIENCE

AWS appreciates that the guidance 'has not been designed as a checklist for cyber resilience minimum requirements.' However, if there are measures that are required rather than recommended, the consistent use of the term 'should' (rather than 'must' for those that are required) throughout the guidance fails to differentiate these.

Part A: Governance
AWS suggests that section A1.8 make clear that the appointed senior executive (eg Chief Information Security Officer) *is accountable for* rather than 'take care of' – cyber resilience issues.

AWS understands the intent of 1.8.2 as drafted, but suggests that the CISO is likely to be involved in internal audits of information security. We suggest revising this statement to reflect that the internal audit team must be independent.

Part B: Capability building
Sections B1.2-1.3 as drafted may suggest that inventories and network maps must be maintained as separate documents and regularly updated. A more efficient approach would be to ensure that the relevant data is available, rather than maintaining separate dataset(s).

Part C: Information sharing
The preamble's reference to 'highly contagious' cyber threats is unsubstantiated and may unnecessarily fuel community concern and confusion.

Part D: Third-party management
The current drafting of Part D perhaps unreasonably characterises the use of third party entities by any organisation as intrinsically establishing cyber risk. Large, complex or matrixed corporate arrangements *may* create more risks for an organisation, but it does not necessarily follow that the risks to an organisation's data or technology are relatively greater merely because of the organisation's use of third party services.

Cyber risks arise from a multitude of factors. Prudent use of third-party services may fundamentally reduce an organisation's cyber risk, not increase it. AWS submits that the first paragraph of Part D should be revised to reflect the fact that the use of third party service providers *may* increase cyber risk but can also be a means by which cyber risk is reduced. This should be particularly observed when the management of cyber risk may not be a core expertise or competency of an organisation. It would be useful for the Guidance to make clear that the fundamental consideration for Boards and Senior Management must at all times be evaluation and management of risk.

AWS further notes that the current draft guidance lacks balance in suggesting that while migrating to cloud 'may present' a number of benefits, using cloud services 'does' bring more challenges. This overlooks the breadth of outsourcing arrangements that are in place for the delivery of any third party technology solution. AWS submits that using cloud services will require a regulated entity to conduct a very similar, albeit specific, due diligence to that which would need to be done for any form of technology outsourcing, including the delivery of on-premise technology.

AWS agrees that the allocation of responsibilities as between parties to a cloud services arrangement, most usually reflected in contract, needs to be precise and clearly understood by all. AWS customers have the option to enrol in an Enterprise Agreement with AWS, which give customers the option to tailor agreements that meet their needs and address regulatory requirements.

While we appreciate RBNZ's concerns around potential concentration risk posed by CSPs, we strongly believe financial institutions can decrease their operational and cyber risk by running well-architected applications on the cloud. Indeed, the cloud helps financial institutions to ensure better operational and cyber resilience than legacy IT systems; and by helping individual financial institutions decrease individual operational risk, address and manage threats, cloud helps ensure stability of the overall financial system and minimize systemic risk.

The robustness of AWS's cloud services and infrastructure, together with our security, services, and tools, help customers to ensure continuity of their services, which is a key prerequisite for financial stability. Further, every customer's workload deployment on AWS is different, which means that virtually no two customers are exposed to the exact same set of technology when using AWS as their service provider. In this sense, AWS can be conceptualized as a set of building blocks that can be combined in infinitely different ways. For example, two customers who run their websites using AWS services will most likely be using different physical data centre buildings, hardware, and different core services to build their solution.

CSPs and the financial services industry share a common interest and responsibility in maintaining operational and cyber resilience. CSPs like AWS make it easier for financial institutions to manage operational resilience than legacy IT systems. Indeed, cloud customers benefit from an infrastructure that is designed for resiliency and integrates multiple levels of redundancy. To avoid single points of failure, AWS minimizes interconnectedness within our global infrastructure. AWS's global infrastructure is geographically dispersed over five continents, with 77 availability zones (AZs) in 24 Regions (For more detail see https://aws.amazon.com/about-aws/global-infrastructure/regions_az/). The AZs, which are physically separated and independent from each other, are built with highly redundant networking to withstand local disruptions. Regions are isolated from each other, meaning that a disruption in one Region does not result in contagion in other Regions. Compared to on-premises environments today, the locational diversity of AWS's infrastructure greatly reduces geographic concentration risk.

Sections D4.2 and D8.6 of the Draft Guidance refer to the substitutability of third parties and the portability and interoperability of data and applications. AWS encourages its customers to evaluate the risks and benefits of all technology options. Whatever the technology solution adopted by an entity, it must plan for events that may have a catastrophic impact on business. Responsible business planning should factor in the probability of foreseeable events and calculate the impact on business outcomes of those events.

Being prepared and able to move entire systems between providers, or moving data to an alternative provider, may be a responsible response to specific events, and it is appropriate that entities be encouraged to consider planning for all such events. This should be the case regardless of what form of technology solution the entity adopts. Data portability and interoperability are relevant issues regardless of the underlying solution adopted to deliver the enabling infrastructure or relevant services. Calling out this issue in a section on Cloud Service Providers undervalues its importance, relevance, and universality.

AWS recommends that Section D8.6 be placed in the general section near to D4.2, and re-written to make its application general.