26 May 2017

Victoria Learmonth
Prudential Supervision Department
PO Box 2498
Wellington 6140
Email: Victoria.Learmonth@rbnz.govt.nz

Dear Victoria,

Amazon Web Services (AWS) is grateful for the opportunity to provide detailed feedback to the Reserve Bank of New Zealand (RBNZ) in regards its technology outsourcing framework for RBNZ-registered banks (Registered Banks). We remain available to provide follow up feedback or meet face-to-face any time to further discuss the issues raised in this submission.

Purpose of this Consultation

This document responds to RBNZ's exposure draft for consultation regarding "BS11: Outsourcing Policy for Registered Banks" dated March 2017 (BS11 Draft). RBNZ has asked for comment regarding "instances where stakeholders believe the wording of the exposure draft is unclear, could be interpreted in more than one way, or differs in substance to what is set out in [the] Final Policy Decisions Document." The first parts of this document provide background on outsourced cloud services, and identify areas where AWS believes additional clarification of the existing language would be useful; the subsequent sections outline some additional items for RBNZ to consider as it finalizes the BS11 Draft.

Background on Outsourced Cloud Services

At its most basic, outsourced cloud computing provides a simple way for financial services institutions to remotely access servers, storage, databases and a broad set of applications over the Internet. A Cloud Service Provider (CSP) such as AWS owns and maintains the network-connected hardware required for these application services, while the end-user Registered Bank provisions and uses what it needs either directly (via an application programming interface by which its independently-operated systems access CSP-maintained data or resources) or via a web application (in which its computing needs are hosted by, and operate on, CSP-maintained resources). The ways in which a Registered Bank can use a CSP are virtually unlimited: primary data storage; back-up and recovery; data analytics and business intelligence; mobile applications; websites and consumer interfaces; front, middle and back-office functionality; and more. Almost anything that a Registered Bank can do on its own systems and equipment, it can do in the cloud.

Cloud computing provides another significant benefit to Registered Banks, RBNZ, and their customers beyond convenience and flexibility: *a global infrastructure that is stable, resilient and secure.* AWS operates data center facilities in multiple locations worldwide ("regions"), which enables the placement of resources, such as applications and data, in multiple locations, and is continuing to expand and add additional regions around the world. AWS's customers can specify where their data and cloud computing resources should be physically located across AWS's regions. Thus, even in cases where AWS does not currently have a region in a particular country, a customer can direct that its data and operations be located in a region that is geographically near its operations (e.g., a bank in New Zealand could store data and conduct operations in AWS's Australia region, since AWS does not currently have a New Zealand region), or that its data and operations be distributed across multiple regions in several parts of the world. This flexibility and redundancy allow AWS and its customers to avoid single points of failure that could compromise a financial institution's ability to function - whether due to weather events, natural disaster, infrastructure (power and water) failures, security concerns or other events – while also maintaining control over where data is stored or processed.

CSPs are also experts at information security, and specifically cloud security. At AWS, cloud security is "job zero"; all AWS customers benefit from data center architecture and network architecture built to satisfy the requirements of the most security-sensitive organizations, including governments and other large financial institutions. AWS provides better security at lower prices for infrastructure[1] than the Registered Banks could likely purchase or assemble on their own.

Specific Responses to the BS11 Draft

1. *RBNZ should clarify that BS11 Applies to Outsourcing Arrangements with Independent Third Parties*

[1] AWS relies on a "Shared Responsibility Model" in which the customer is responsible for the security "of the cloud" and AWS is responsible for security "in the cloud". The financial institution, rather than AWS, determines what content it stores in AWS, controls how it configures its solution, and how it secures its content, including what security features and tools it uses and how it uses them. For these reasons financial institutions also retain responsibility for the security of content they store in AWS, or other IT they use with their AWS infrastructure, such as the guest operating system, applications on their computing instances, and content stored and processed in AWS storage, platform and database services. AWS is responsible for managing the security of the underlying cloud environment. Its services are content agnostic, in that they offer the same high level of security to all customers, regardless of the type of content being stored, or the geographical region in which they store their content. AWS's world-class, highly secure data centers utilize state-of-the art electronic surveillance and multi-factor access control systems. Data centers are staffed 24x7 by trained security guards, their locations are not disclosed internally or externally except on a need-to-know basis, and access is authorized strictly on a Least Privileged basis.

On its face, the BS11 Draft applies to Registered Banks that wish to outsource functions to a non-New Zealand parent or related party bank. Curiously, the document does not contain parallel for outsourced arrangements with independent third parties. For example, Section 4.1 outlines various requirements for a bank that wants to outsource functions to an overseas parent or related party, but there is not a parallel set of requirements for banks that want to outsource functions to an independent third party, even though the Final Policy Decisions Document contemplates arrangements with independent parties.[2]

To ensure that Registered Banks clearly understand their obligations when entering into outsourcing arrangements with independent third parties, RBNZ should amend BS11 so that it clearly applies to outsourcing to independent third parties.

2. *RBNZ should clarify its expectations when a Registered Banks enters into agreements with independent third parties*

Assuming that RBNZ agrees with AWS's proposed clarification above regarding the BS11 Draft, RBNZ should also provide more detail regarding what is specifically required of a Registered Bank when it enters into an outsourcing arrangement with an independent third party. As noted above, the BS11 Draft gives extensive guidance when the outsourcing arrangements are between related parties, but provides little guidance on arrangements with independent third parties.[3] Without such a framework, it will be difficult for a Registered Bank. We note that the guidance needn't be highly specific, and that a principles-based regulatory framework would allow flexibility for the Registered Banks to develop solutions that are appropriate to the bank's needs while still meeting the RBNZ's regulatory mandate.

3. *RBNZ's requirements for Registered Banks who outsource to Related Parties may inadvertently preclude the Related Parties from using outsourced cloud services.*

---

[2] The Final Policy Decisions Document states that "[f]or all arrangements with an independent party banks must ensure that they fully comply with the outsourcing policy requirements, but they will not require Reserve Bank non-objection before entering into an arrangement"

[3] The only statement on a Registered Bank's obligations when outsourcing to independent third parties is RBNZ's guidance on Section 4 of the BS11 Draft, which incorporates paragraph 21 of the Final Policy Decisions Document ("[f]or arrangements with independent third parties banks will be able to rely on the robust disaster recovery/business continuity preparation requirements provided by the independent service provider"). The BS11 Draft itself, however, does not contain language stating as such. As a result, it is unclear if this sentence constitutes binding guidance under the plain language of the policy. Even if it is binding guidance, the requirement described there remains vague, since the policy does not provide guidance on what "robust disaster recovery/business continuity preparation requirements" means, or how to evaluate whether a third party's DR/BCP requirements are sufficiently "robust" to satisfy the policy.

As noted in the background description above, there are substantial benefits to using an outsourced cloud computing infrastructure over a physical infrastructure that is built, maintained and operated by a Registered Bank on its own. While we understand the concerns articulated by the RBNZ regarding the potentially complex issues that may arise between a Registered Bank and an overseas parent or related party in the event of a disruption, several of the requirements contained in the BS11 Draft would, on its face, make it impractical or impossible for a Registered Bank to realize the benefits of cloud computing if the parent or related party solution itself involves an outsourced cloud computing infrastructure. In particular, BS11 states that a Registered Bank must maintain a back-up system over which it has "legal and practical control". On its face, that requirement seems to say that a Registered Bank must build, maintain, test, and operate its own data centers and computing operations that can be accessed and brought on line within hours of an interruption overseas, or else maintain a fully redundant outsourced solution of its own (where it has a direct relationship with the third party provider). But if that's the case, either of these solutions would effectively undo the benefits of outsourcing, and are a strong disincentive for the Registered Bank to consider outsourcing in the first place. To resolve uncertainty, the RBNZ should clarify the meaning of "legal and practical control" in the context of related party arrangements where the related party uses (or wants to use) an outsourced cloud solution.

Suggestions Regarding Additional Guidance for Outsourced Cloud Computing

In the event that RBNZ determines to reopen the BS11 Draft or issue additional information or clarifications specifically regarding outsourcing for cloud computing and storage, AWS suggests that the following information may be a useful starting point for such guidance:

As described above, cloud services offer Registered Banks several benefits, including allowing Registered Banks to control their content and security, while accessing technology and infrastructure that can reduce their costs and deliver *increased* security, reliability, and availability compared to on-premise IT systems or traditional outsourcing models.

1. *Objective for Outsourcing Guidelines*

To ensure that Registered Banks can use and benefit from technology that helps their business and compliance efforts, it would be important that any outsourcing guidelines strike the right balance between implementing a prudent approach to technology risk management (TRM) and introducing new requirements that would be outright restrictive of a technology.

We are mindful that RBNZ previously promulgated guidelines on outsourcing technology in 2006. Although those guidelines were thorough and relevant to the outsourcing landscape when issued, the landscape for cloud computing in particular has since changed significantly since then, such that Registered Banks can now seamlessly integrate cloud computing into core and day-to-day operations.

Meanwhile, the ability to ensure the safety and integrity of mission-critical data stored in the cloud and computing processes performed in the cloud has never been greater.

Different outsourcing models have different implications for TRM, because the relevant level of control each of the Registered Bank and CSP exercise over the IT security measures, the IT solution and the content stored in or processed using that solution will differ in each model. Registered Banks today can choose from a spectrum of outsourcing models, ranging from Infrastructure-as-a-Service (IaaS) offerings that provide core infrastructure, to full 'managed service' IT outsourcing arrangements. In addition, while offerings may appear similar, or be called similar things, there may be substantial differences in the way the relevant services are structured. This means that customers may retain varying degrees of control over their security, solutions and content depending not only on the type of outsourcing model used but also on the particular cloud deployment model (or other) offering they choose.

The agreement between a Registered Bank and the CSP should allocate responsibilities based on the actual level of control exercised by each party over the relevant security, solution and content. For example, a Registered Bank that uses an IAAS offering decides and controls how to use that infrastructure to architect an IT solution and what IT security measures to deploy as part of that solution. The Registered Bank also retains control of content stored in or processed using that solution. At the other end of the scale, in a 'managed services' model, the CSP would exercise much greater control over determining and implementing IT security measures, the architecture of the IT solution, and the content stored in or processed using that solution. **See Appendix B for AWS Shared Responsibility**.

2. *Scope and Applicability of Outsourcing Guidelines*

There are typically two approaches to guidance from a regulator: prescriptive and proscriptive. Prescriptive regulation states affirmatively what a regulated entity should or must do, and the presumption is that a regulated entity's failure to do the thing prescribed constitutes an enforceable violation of the regulation or rule. Proscriptive regulation, by contrast, establishes limits on what a regulated entity may do, and the presumption is that, as long as a contemplated activity or practice by the regulated entity stays within the regulatory limits, the regulated entity does not need explicit permission from the regulator to take action. A simple way to think of this difference is that in a prescriptive system, anything that isn't explicitly permitted is prohibited; in a proscriptive system, anything that isn't explicitly prohibited is permitted.

We believe that if RBNZ reopens BS11 to provide additional guidance regarding cloud-service outsourcing, RBNZ should adopt a proscriptive standard, rather than relying on a "white list" of permitted activities as it has done with respect to outsourcing among related parties. We strongly believe that it would be more efficient (since capabilities are constantly changing) for RBNZ to outline principles that describe its concerns and tolerances, and then allow Registered Banks and CSPs to

determine how to structure solutions that address RBNZ's concerns while staying within the tolerated limits. By establishing minimum standards, and allowing participants to negotiate terms that will meet their economic and business needs within that framework, RBNZ will encourage innovation and competitiveness while also ensuring the safety and security of data and infrastructure that powers the New Zealand financial system.

Conclusion

AWS appreciates the opportunity to discuss these matters with RBNZ. AWS believes that it is a good thing for RBNZ and the Registered Banks that it oversees to update the RBNZ existing guidelines on outsourcing. Doing so will enable New Zealand's Registered Banks to compete globally by taking advantage of a state-of-the-art pay-as-you go infrastructure; implement a robust security framework that is richer and more secure than the Registered Banks could likely assemble on their own, and with safeguards and checks built in that will allow Registered Banks to demonstrate compliance; and preserve for RBNZ the ability to effectively access data information that it needs to carry out its regulatory priorities without compromising data integrity or security.

Yours sincerely

(signed)
Roger Somerville,
Head of Public Policy, APAC
Amazon Web Services

Appendix A: Proposed guidance relating to third-party audits and reporting in lieu of direct audits by a Registered Bank or RBNZ

If an CSP already follows a rigorous and regular audit and reporting program, RBNZ guidelines for outsourcing should provide that third-party audits and reporting by the CSP are an acceptable approach to validation in lieu of direct audits by the Registered Bank, provided that the program meets minimum standards defined by RBNZ. These minimum standards should include ensuring that the program:

- is carried out by professional independent auditors of repute;
- is carried out against objective international standards, such as ISO27001, SOC 1, SOC 2, MTCS Level 3 and PCI-DSS or alternative future standards that supersede or are substantially equivalent to those standards;
- results in provision of independent audit reports that are available directly to the Registered Bank, and may be provided by the Registered Bank to the RBNZ; and
- involves such audits and reporting at a minimum frequency specified by RBNZ.

Appendix B: Shared security responsibility

AWS acknowledges the importance of IT as a key enabler for business strategies, and its platform has been architected to enable customers, including Registered Banks, to achieve greater flexibility, increased resilience, and reduce their costs. In support of these goals, AWS has adopted a Customer/AWS Shared Responsibility Model. This model enables customers to achieve secure, robust, cost-effective, and flexible IT solutions that could meet RBNZ's objectives for TRM.

Security in the cloud is different from security in an on-premise data center. When using a cloud service to host data and applications, security responsibilities are shared between the CSP and the Registered Bank. The CSP is responsible for securing the underlying infrastructure that supports the cloud, while the Registered Bank is responsible for the things that it puts into the cloud or that connect to the cloud. Put another way, AWS is responsible for the security OF the cloud; the BSI is responsible for security IN the cloud. AWS protects the global infrastructure that runs the services offered in the AWS cloud. This infrastructure is composed of the hardware, software, networking and facilities that run AWS services, including "managed services" (services that provide the resources a Registered Bank needs in order to perform a specific task).

The Shared Responsibility Model is shown below:

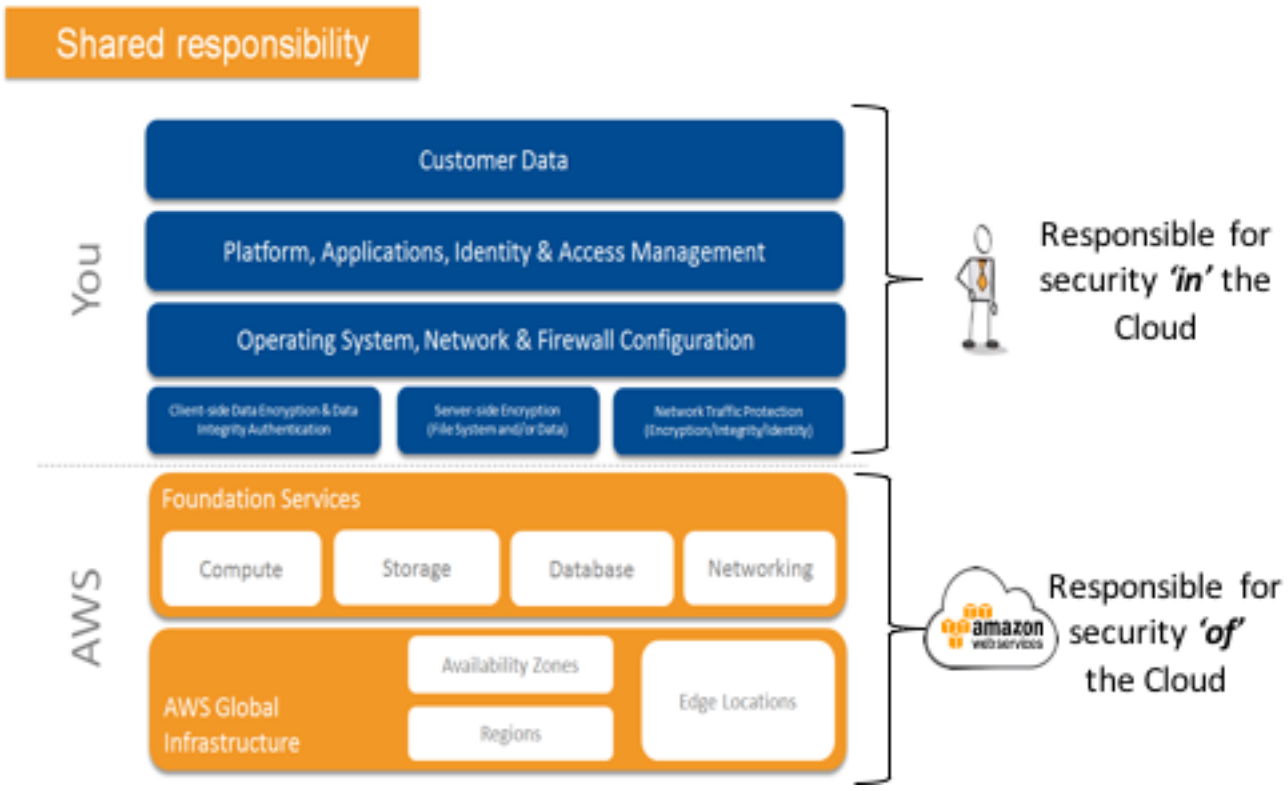

Figure 1: Shared Responsibility Model

Under the Shared Responsibility Model, AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the AWS services operate. The customer is responsible for management of the guest operating system (including updates and security patches to the guest operating system) and associated application software, as well as the configuration of the AWS provided security group firewall and other security-related features. This division of control and responsibility is very important for understanding why a "One Size Fits All" approach to outsourcing agreements is not appropriate for the different outsourcing models in use today.