Microsoft Pty Ltd

Australian Financial System Inquiry: Response to request for further submissions

August 2014

Response in relation to Chapter 9 of the Interim Report

Microsoft is pleased to respond to the Inquiry's request for further submissions in relation to its consultation on technology and specifically to the request for further information noted in the interim report in relation to regulation, legislation and the regulatory regime governing the use of cloud technology by the financial services sector (Chapter 9).

As such we are very supportive of this Inquiry's observations in the Interim Report that:

> *Technological innovation is a major driver of efficiency in the financial system and can benefit consumers. Government and regulators need to balance these benefits against the risks, as they seek to manage the flexibility of regulatory frameworks and the regulatory perimeter. Government is also well-positioned to facilitate innovation through coordinated action, regulatory flexibility and forward-looking mechanisms.*

We feel that the Inquiry could take a further step of recommending an approach that enables this coordinated approach and regulatory flexibility particularly as it relates to cloud computing.

The interim report clearly identifies the great potential of cloud technology to improve the efficiency, productivity and innovation within the financial services sector. Cloud computing offers financial institutions new avenues for greater flexibility, scalability and agility as a result of more efficient resource utilization. That said, we also note in realising these benefits, financial institutions (FIs) and cloud services providers (CSPs) need to ensure compliance, security and performance standards are well documented and addressed.

This submission seeks to find that balance by sharing our experience as one of the leading cloud service providers to the financial services sector, and from our interaction with regulators, policy makers and customers around the world. We have also outlined a way forward through a principles-based framework for regulators, financial institutions and CSPs to consider.

Key considerations for future cloud regulation framework

As a leading supplier of information technology to the financial services sector, Microsoft has actively sought the views and concerns of the industry and its regulators across the Asia Pacific region. This submission reflects these discussions.

Given both the fast pace of change and the shared interest that the cloud services industry and their financial services customers have in a trusted cloud computing environment, we strongly advocate a flexible, principles-based approach to cloud technology, as has been adopted by a number of other regulators in the region, in relation to both cloud computing and privacy requirements. In contrast to proscriptive legislation, regulatory guidelines that take a principles-based approach will allow a combination of regulation and industry self-management, with regulators potentially setting out best practice on key industry issues such as compliance,

privacy and data security. Additionally, a principles-based approach provides for changes in both the technology and the emerging policy and compliance environments.

In terms of the current regulatory framework for cloud computing services, we have found that most global financial regulators, including APRA, tend to rely on existing regulations and guidelines on outsourcing, data risk management, technology risk management and business continuity management. The absence of clear guidance beyond the existing outsourcing regulations will eventually hinder the potential of cloud computing, particularly in a highly regulated and security-sensitive industry such as financial services.

This Inquiry presents an opportunity to mark a clear difference from the first wave of outsourcing by the financial institutions in the 1990s, and to establish a system in which collaboration between financial institutions, service providers and regulators promotes trust, transparency and innovation from the outset.

We believe that a set of guiding principles along the lines of those attached would provide greater clarity and guidance for safer and wider cloud adoption in the financial services industry, enabling customers to benefit from innovation, greater efficiency and increased competition, without exposing them to greater risk.

It is important that the guiding principles ensure:

1. a full due diligence process be undertaken when assessing vendors;
2. compliance checks and regular monitoring and audits are established;
3. confidentiality and security standards are addressed;
4. data location and transparency is considered;
5. data segregation and data use limits are required; and
6. sub-contractor and termination requirements are agreed up front.

We understand that the configuration and architecture of cloud computing services will vary greatly from CSP to CSP and not all solutions will be able to meet all the principles as recommended for the financial services industry. As such, the proposed principles will greatly help the financial services industry to be better prepared, to have a clearer understanding of the relevant industry requirements and to make the right decisions, when assessing different cloud offerings.

Why we support a principles-based approach to regulation

Cloud computing has an enormous potential to bring significant advantages to individuals, businesses and public administration. It remains a rapidly advancing field and in our experience a principles based approach has better prospects of remaining relevant and inclusive in the face of rapid development, while continuing to encourage innovation, than a proscriptive approach. A principles based approach is also more suitable to adoption beyond the Australian domestic market, as it allows for regional interpretation and is thus better placed to provide the basis of

broader regional best practice. As Australia and its financial institutions increasingly play a pan-regional role in financial markets, and seek to grow this further, this is an important consideration.

In addition to being a more flexible approach, we also believe the principles based system is likely to be more readily agreed and formulated by the numerous interested parties than a more detailed or proscriptive rules based approach. We believe we have gone some way to demonstrating this practical advantage by the significant work we have already done on this specific topic with the various stakeholders. To date, we have convened a focused discussion between FIs, CSPs, financial regulators and industry bodies, and have drafted **10 Safe Cloud Principles** (please refer to the Appendix for a copy) which will we believe will provide a useful contribution towards the creation of a unified, condensed and clarified set of best practices for cloud in FSI regulatory guidelines.

By providing a draft set of principles already viewed as fit for purpose, we hope not only to give a detailed insight into the priorities of the industry, but also to provide a concrete basis for further discussions of the principles based approach, and in so doing save significant time for all parties.

The Safe Cloud Principles we have set out below cover key requirements such as confidentiality, availability and integrity and are derived from the laws, regulations and guidelines with which FIs must comply under the current applicable framework.

1. **Service provider reputation and competence**: FIs must carry out, and CSPs must assist in facilitating, a risk assessment and due diligence on the CSP to ensure that the CSP and its cloud services meet the legal, regulatory, contractual and business requirements. FIs should have in place a risk management plan that includes measures to address the risks associated with the use of cloud services.
2. **Review, Monitoring and Control**: Compliance does not end at signature of the contract. CSPs must provide regular reporting and information to demonstrate continued compliance with the legal, regulatory, contractual and business requirements throughout the duration of the contract. FIs and CSPs must meet regularly to review the reports and performance levels. The contract must provide for an effective mechanism for remedial actions arising from any issues that emerge or non-compliance.
3. **Audit**: CSPs must provide FIs and applicable Financial Regulators with audit rights.
4. **Confidentiality and Certified Security Standards**: CSPs must be certified to have and maintain robust security measures and comprehensive security policies that meet or exceed international standards (ISO27001 accreditation should be a minimum). CSPs should use encryption technology that meets or exceeds international standards to help protect and secure the FI's data at all times.

5. **Resilience and Business Continuity**: The cloud service must be reliable. CSPs must have an effective business continuity plan with appropriate service availability, recovery and resumption objectives and with regularly tested and updated procedures and systems in place to meet those objectives. The risks of downtime should be minimised through good planning and a high degree of system resilience.
6. **Data Location and Transparency**: CSPs must disclose exactly where data will be located. FIs should ensure that the government policies, economic and legal conditions of the identified locations are safe and stable.
7. **Limits on Data Use**: CSPs should not use FI's data for any purpose other than that which is necessary to provide the cloud service. The contract should prevent CSPs from using FI data for any secondary purpose.
8. **Data Segregation/ Isolation**: FI customer data must be segregated (whether via logical or physical segregation) from other data held by the CSPs. CSPs must be able to identify the FI's customer data and at all times be able to distinguish it from other data held by the CSP.
9. **Conditions on Subcontracting**: CSPs should only use subcontractors if the subcontractors are subject to equivalent controls as the CSP.
10. **Conditions on Termination**: FIs must have appropriate exit provisions in the contract with the CSP. To the extent that the FI requires, on termination, the CSP must work with the FI to return the FI's data to the FI and then the CSP must permanently delete the data from the CSP's systems. Any data that does not need to be returned to the FI must be permanently deleted by the CSP. This is particularly important considering the history of challenges around termination under more traditional forms of outsourcing.

These Safe Cloud Principles are intended not only to capture the broad principles underlying current regulation but also to drive adoption of what we perceive to be current global best practice. Specifically the above principles are compatible with *The Australian Prudential Regulation Authority (APRA) Outsourcing Standard*, *APRA Outsourcing Guide*, *APRA Data Risk Guide*, *APRA Security Guide* as well as *The Australian Privacy Principles*.

The interim report clearly highlights some risks associated with the rapid cloud adoption in the financial services sector, including control of data, data management under subcontractors, and the concentration risk on a system-wide basis. We believe that the proposed key principles above provide a robust means to address these key concerns, and we set out the principles that address each key concern in the table below for your reference:

Risk identified in the interim report	**Safe Cloud Principles that addressed the concerns**

How to ensure FI's control over their data and systems	Principle 6, 7, 8, 10
How to govern data if located offshore	Principle 6
How to monitor the concentration risk on a system-wide basis	Principle 1, 2, 3, 4, 5
How to manage data if it is under subcontractor	Principle 9, 10

Suggestions for the next steps

It is clear that transition to the cloud is becoming a major trend as the traditional barriers for the move are being addressed, in part as a result of the willingness of CSPs to tailor their cloud offerings to meet FSI needs and regulatory requirements.

Government and regulators have an important role to play in facilitating the adoption of cloud computing in Australia by expediting government and industry collaboration to clarify and agree clearer guidance beyond the existing legislation and regulation. In addition, regulators have a real opportunity to collaborate with industry, including associations, academics and CSPs, to define best practice standards for ensuring security and compliance within the context of cloud adoption in the financial services industry.

In summary, we strongly support a principles-based approach to setting out clearer guidance governing cloud adoption in the financial services sector, so that customers and the industry have a framework within which to structure their adoption of cloud based solutions.

We believe that starting with cloud computing, this principles-based approach could also provide a good framework for the industry and regulators to assess the risks and benefits of other new technology and business models, including big data and new payment platforms.

As a key next step, we request the Inquiry to assess the principles based approach (and the attached Safe Cloud Principles), and we would welcome further cross-industry discussions to build on our work to date. We would also welcome the opportunity to meet with the Secretariat to outline the Safe Cloud Principles as we well as share the insights from our interaction with financial series regulators in Asia Pacific and across the world.

Appendix: Safe Cloud Principles document.