CSC’S POINT OF VIEW ON THE PRACTICAL APPLICATION OF CLOUD MANAGEMENT IN LINE WITH FINANCIAL REGULATOR GUIDANCE

In response to the increased usage of cloud-based services by regulated entities, the Australian Prudential Regulatory Authority (APRA) has released an Information Paper: Outsourcing Involving Shared Computing Services (including Cloud), dated 6 July 2015.

The paper focusses on the weaknesses observed by APRA in how regulated entities consider, manage and govern the risks of using shared computing services (SCS), and it provides guidance for addressing these weaknesses.

In order to manage the use of SCS in accordance with APRA guidance, Financial Institutions should develop a clearly defined strategy for migrating to an SCS model; implement effective governance measures; ensure ongoing consideration of security and recovery risk; and implement ongoing third party assurance arrangements.

WHAT DOES THIS MEAN FOR REGULATED INSTITUTIONS?

Provided that regulated entities demonstrate sound risk management and governance practices in line with APRA’s guidance, the use of shared computing arrangements with low and heightened inherent risk ratings is permitted.

CSC POINT OF VIEW

CSC believes that regulated entities can pragmatically implement a framework for managing outsourcing of computing services in line with APRA guidance, by leveraging organisational capabilities that already exist as a result of compliance with other APRA requirements.
Who is responsible? Accountable? How do we manage risk?

Good governance is instrumental to the successful implementation of SCS. It provides the structure, responsibilities, competencies, reporting and risk management processes for managing SCS.

Organisations must therefore establish an overarching governance capability that enables decision making in line with company and regulatory requirements throughout the SCS life cycle.

CSC has developed a framework for adopting SCS in line with APRA guidance. The framework consists of 6 consecutive stages, with an additional component for Governance that runs across all of them.

This framework is derived from our experience working with APRA-regulated entities, as well as our expertise in risk management and extensive hands-on experience as a cloud service provider.

1. Governance

Who is responsible? Accountable? How do we manage risk?

Good governance is instrumental to the successful implementation of SCS. It provides the structure, responsibilities, competencies, reporting and risk management processes for managing SCS.

Organisations must therefore establish an overarching governance capability that enables decision making in line with company and regulatory requirements throughout the SCS life cycle.

2. Business & Technology Strategy Alignment

What can we do to support both operational and technology strategic objectives?

To achieve long-term success in a complex operating landscape, organisations must develop mutually supportive operational and technology strategies, based on an objective understanding of the risk environment and the organisation’s ability to manage these.

3. Risk Assessment of Options

What are the options? What will happen to our operational and technology risk profiles?

Financial Institutions must pro-actively identify and manage the risks that materialise or increase as a result of the change initiative. A risk-based view of the options will enable the organisation to choose the solution and associated risks that are within the organisation’s risk appetite and ability to manage.

4. Vendor Risk Management

Who will we partner with?

When selecting vendors, the organisation must ascertain how well the vendor manages its own operational and technology risks. This includes an understanding of the vendor’s information security management and business resilience capabilities.

Demonstrable outcomes:

- Proposals for change link back to clearly defined business and technology strategies
- Business case includes consideration of benefits and risks alike

Demonstrable outcomes:

- Risk management framework defining risks, impact types and tolerances, risk appetite and risk governance structure
- Comprehensive current state and post-transformation risk and control profiles
- Chosen solution(s) aligned to desired enterprise architecture

Demonstrable outcomes:

- Vendor management framework including vendor risk and control assessment criteria and tolerances, assurance requirements and operational oversight
- Vendor due diligence conducted against the established criteria
Demonstrable outcomes:

- Governance framework with clearly defined roles and responsibilities, levels of authority and delegation
- Processes for identification, management and timely review of SCS-related risks.

Financial Institutions remain responsible for managing the risks associated with SCS, such as the unavailability of IT systems and data. In other words: You can outsource the service, but you can’t outsource the risk.

The transformation must include development or enhancement of controls that enable the organisation to manage such risks post-implementation.

With technology outsourcing comes a high reliance on the SCS’s technology resilience — the IT environment’s ability to ‘absorb’ disruptions to components and remain available.

Organisations must maintain a capability that enables it to meet business objectives in the event that the supplier has become unavailable.

It’s often not practical to apply a rigorous assurance program over material suppliers. This is particularly true for SCSs who provide services to hundreds of regulated entities. Organisations could consider implementing a collaborative assurance model in partnership with multiple customers. The level of assurance review should be commensurate with the level of risk the organisation is exposed to.

Demonstrable outcomes:

- Proposals for change link back to clearly defined business and technology strategies
- Business case includes consideration of benefits and risks alike

Demonstrable outcomes:

- Risk management framework defining risks, impact types and tolerances, risk appetite and risk governance structure
- Comprehensive current state and post-transformation risk and control profiles
- Chosen solution(s) aligned to desired enterprise architecture

Demonstrable outcomes:

- Vendor management framework including operational oversight, risk management and assurance
- Schedule of assurance testing, including assessment of all aspects of the IT security environment over time

INDUSTRY PERSPECTIVE: GOVERNANCE, RISK & COMPLIANCE | 3

RECOMMENDATIONS

APRA recommends the following practices to be adopted:

- Engaging risk, security, outsourcing and assurance functions
- Alignment between business and technology strategies
- Systematic and comprehensive due diligence process for selecting solutions and services
- Comprehensive assessment of delivered risk
- Ongoing management of delivered risk, including management of material service providers
- Consideration of risks and controls to manage business disruption
- Assurance activities that are appropriate for the level and type of risk associated with the SCS
HOW CSC CAN HELP

CSC can offer a comprehensive solution to assist Financial Institutions in meeting the guidance of the APRA paper.

With deep industry experience, CSC’s consulting capability covers all aspects of technology outsourcing risk management and governance, including design and review of cloud security controls.

CSC also provides cloud hosting services and cloud-based solutions that have been adopted by Financial Institutions across the globe.

CSC offers an ‘as a service’ model which combines cloud services with a fixed consulting fee each month/quarter. Both cloud and consulting services can be up- and down-scaled as required.

ABOUT THE AUTHOR

Catherine de Ruyter de Wildt leads CSC’s Governance, Risk & Compliance consulting practice in Australia and New Zealand. She works with business leaders to develop and implement risk and compliance management frameworks and support the execution of strategic change programmes to enhance organisations’ operational and technology risk management capabilities.

Ms. de Ruyter de Wildt has both a consulting and banking background, having worked for one of the global Big Four consulting organisations, as well as for one of Australia’s Big Four banks.

For more information, contact: cderuyterdew@csc.com

ABOUT CSC

CSC is a global leader in next-generation IT services and solutions. The company’s mission is to enable superior returns on our clients’ technology investments through best-in-class industry solutions, domain expertise and global scale. For more information, visit us at www.csc.com.