# Prudential Regulatory Risk Governance of IT Multi-Sourcing Strategies within the Australian Banking Sector

Brian Strong
School of Business
University of Southern Queensland
Toowoomba, Queensland
Email: U1042749@umail.usq.edu.au

Professor Aileen Cater-Steel
School of Business
University of Southern Queensland
Toowoomba, Queensland
Email: Aileen.Cater-Steel@usq.edu.au

Dr Michael Lane
School of Business
University of Southern Queensland
Toowoomba, Queensland
Email: Michael.Lane@usq.edu.au

## Abstract

*Banks employ different IT sourcing strategies to reduce IT costs. Australian banks are highly regulated by the Australian Prudential Regulatory Authority (APRA). We selected the two largest Australian banks, Westpac Banking Corporation (WBC) and Commonwealth Bank of Australia (CBA) to investigate the complexity of their IT multi-sourcing models and associated risks. We analysed public documents to reveal the IT sourcing trends from 2009 to 2013, and compared the alignment of the banks' risk frameworks with the APRA risk framework. Finally we reviewed APRA's risk management at the finance industry level and identified that neither risk management nor governance is performed and/or reported by APRA to the Reserve Bank of Australia. Therefore to ensure the cumulative effect of the banks' IT sourcing strategies are measured and reported at the industry level, it is recommended that APRA develops and implements an industry-level risk framework mirroring standard APS 115.*

**Keywords**

IT multi-sourcing, offshore-outsourcing, operational risk, Australian banks, Australian Prudential Regulatory Authority.

## INTRODUCTION

The Australian Financial Services Industry (AFSI) manages AUD$4,900 billion worth of assets. The banking sector within the AFSI comprises 56 Authorised Deposit-takers Institutions (ADIs) (12 domestic and 44 foreign owned banks) that manage 55.9 percent (AUD$2,724 billion) of the AFSI assets. In the banking sector, the four major banks manage approximately 77 percent (AUD$2,000 billion) of the value of the assets within the AFSI. The remaining 23 percent (AUD$724 billion) is managed across eight smaller domestic banks and 44 foreign owned banks with a local presence in Australia (Australian Trade Commission 2011). From the four major domestic banks we have selected Westpac Banking Corporation (WBC) and Commonwealth Bank of Australia (CBA) for our case studies, as they are the two largest banks by capitalisation within the AFSI.

The AFSI is a highly regulated industry governed by the Australian Prudential Regulatory Authority (APRA) as legislated by the Banking Act 1959 (Australian Government 1959) to perform a governance role and enforce adherence to the Australian Prudential Standards (APS). APRA provides guidelines to the banks on managing all aspects of their business that may have the potential to impact customers and the economy.

Although profitable, the banks are under pressure from the market to reduce their cost to revenue ratio. One of the main cost reduction strategies the banks employed was to reduce IT costs by outsourcing IT services. Subsequently a trend has evolved over the last five years with the banks offshore-outsourcing IT services to achieve further cost savings. This has resulted in a mix of delivery models (multi-sourcing) used to deliver IT services.

**Research Problem**

Concerns have been raised as to whether the use of APS regulations is adequate to manage the risks associated with the banks' IT multi-sourcing strategies and the potential impact on the economy if a catastrophic event were to occur with one or more of the banks' core banking systems.

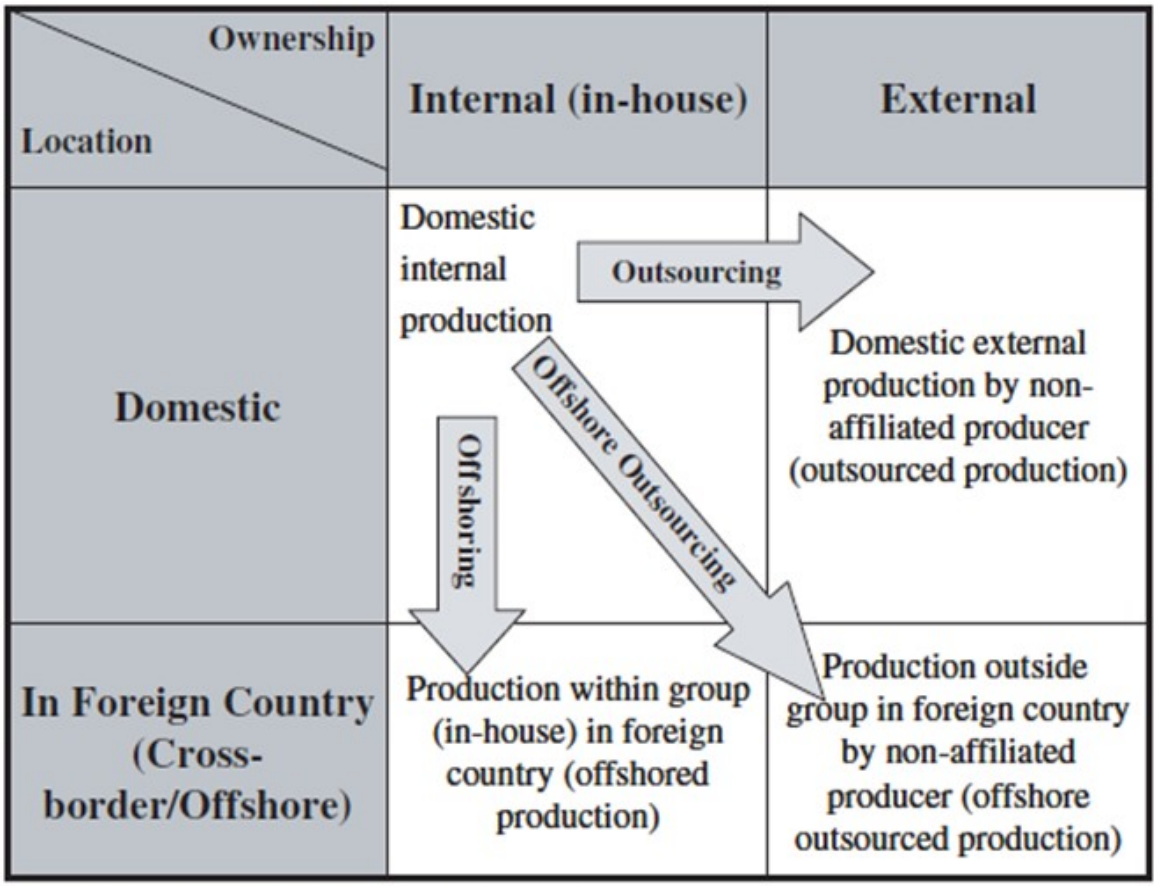
Consider an example of a potential catastrophic scenario: the IT payments system fails at one of the banks and the overnight processing of payments cannot be performed. The bank cannot recover the system and complete the payments run. None of the other banks are able to assist by executing the payment runs on their systems because their operations are delivered from a different external service provider at an offshore location. In the past while these services were outsourced the resources were available locally and did perform the payment run for the bank that failed. It should be recognised that all government payments, domestic and international, all business transactions both domestic and international, all salary, all personal payments would not be transacted. This could lead to dire outcomes with government, business and individuals defaulting on loan payments.

This paper is structured as follows. After a brief review of the prior research, the methodology is described. The data analysis section reports the findings and these are discussed. The conclusion summarises the answers to the research questions, states the research limitations and provides recommendations to APRA regarding a more comprehensive risk model.

## RELATED RESEARCH

**Sourcing Models**

For the purpose of this study, we adopted the standard sourcing matrix illustrated in Figure 1. This diagram was created by UNCTAD and applied by Kirkegaard (2008) to explain the relationship between outsourcing, offshore-outsourcing and offshoring.




*Source*: Adopted from UNCTAD (2004, Table IV.1).

Figure 1. The Sourcing Matrix (Kirkegaard (2008)

Figure 1 presents four distinct models to deliver services: in-house; outsourcing; offshore-outsourcing and offshoring.

### Risk Management

From an operational risk perspective APRA implements the guidelines detailed in the Basel II capital accord produced by the Basel Committee on Banking Supervision (BCBS). The BCBS defines operational risk as "*risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk*" (2004).

In a paper on risk and governance within UK banks, Alexander (2006) referred to "*the principal-agent model which generally is concerned with how one individual (the principal) can design a contract which motives another person (the agent) to act in the principal's interest*" (2006). The principal-agent model is based on agency theory (Eisenhardt (1989) to explain the relationships where a company uses a third party to deliver products or services on their behalf. One of the reasons Alexander stated a company uses an agent is to attempt to move risk to the third party. Alexander reviewed the systemic risks that *the principal-agent model* can cause, not only to the banks, but also the economy as a whole: "*Systemic risk can also arise from problems with payment and settlement systems or from some type of financial failure that induces a macroeconomic crisis*" (2006). Alexander supported this statement by linking it to the Basel Committee statement on the importance of corporate governance within the banking industry to aid national and global economic stability.

The next step in reviewing risk management of the banks' IT service when using multi-sourcing as a delivery strategy is to identify the models used to measure and manage risk impact within the banking sector. Terry (2009) outlined the main methods of measuring risk and allocation of a capital value to the risk within the AFSI. Terry discussed three categories of risk: credit, market and operating. In this study we focus purely on the operating risk category as this is where IT systems, processes and people are included in the risk calculation for each bank's risk profile and capital allocation. Within operating risk the Basel Committee has identified and recommended three methods to calculate risk capital allocation: Basic Indicator Approach (BIA), Standard Approach (SA) and Advanced Measurement Approach (AMA). Effective from the 1st January 2008 both CBA and WBC were approved to use AMA and APS 115 (APRA 2013). APS 115 articulates the advanced measurement of calculating capital adequacy and also the risk framework that Authorised Deposit-taking Institutions (ADIs) must adhere to in order to meet the Basel and APRA requirements.

### Research Questions

Previous research into IT sourcing models, risk management and governance raise the following research questions which are answered by analysing documents available in the public domain:

RQ1. Do the banks employ multi-sourcing solutions to deliver their IT services?
RQ2. What are the risk governance model/s used by the banks to manage risks associated with their IT services multi-sourcing strategy?
RQ3. Is the industry level IT operational risk exposure adequately managed by APRA?

## METHODOLOGY

### Research Approach

This study is based on a five year longitudinal case study of two banks in the AFSI. The risks associated with IT multi-sourcing were identified and analysed for each bank using the following approach. First we determined if the current risk and governance frameworks published by APRA are used in each bank. Secondly we determined whether the risk and governance frameworks within each bank manage these risks at an acceptable level for the bank and for the economy as a whole.

To achieve these results the author used a technique of content analysis to complete the analysis. The author built frequency queries to extract quantitative data on the use of themes, and then identified the sections and the context in which the theme was used. This process enables the researcher to apply inductive inference based on the questions defined above (Krippendorff 2013).

Document analysis strategy was considered to be appropriate for this research because data was obtained from sources that have been verified by either an independent auditor, government regulator or an 'officer of the bank'. The primary approach to the collection of data for this research was to collect qualitative information in the public domain made available by the banks, APRA, and BCBS on their websites. Qualitative data is in the form of bank annual reports, APRA and BCBS regulatory documents, and media releases from the banks published in the Australian media. The approach used in this study takes a similar approach to that of Guthrie et al. (2004) on intellectual capital reporting. Guthrie et al. also used annual reports to carry out the content analysis to show how the companies in their sample utilise intellectual capital reporting. In an overview of content analysis produced by Stemler (2001), he performed an assessment, research and evaluation of the use of content analysis as a technique in conducting research. Stemler found through his study that content analysis is a

powerful technique but that to make it successful the definitions of the themes or categories need to be well defined. As part of the construction of the NVivo queries, Stemler's advice was followed. Stemler's findings have also been supported by Strijbos et al. (2006) in their paper that focused on computer-supported collaborative learning. The main issue they identified was to ensure the definitions and themes are well defined to ensure the research produces relevant output.

For this study having more than one source for delivering IT services is viewed as complex. The reason for this stance is more than one source requires more than one commercial agreement which leads to more than one governance forum. Each of these governance forums may require internal governance staff with different levels of experience e.g. higher legal/commercial as opposed to delivery/operational. One could debate the levels of complexity but the constraints of the paper do not allow for a broader discussion.

The '*Component of Risk Management*' listed in Table 3.4 was derived from the category 2 list in attachment E (Loss event categories) of APRA's operational risk prudential standard (APRA 2013). Operational risk covers all aspects of the banks' business that support the customer facing business units and therefore covers more than technology and IT sourcing. For this study, the risk management components list is restricted to those category 2 risk management components that relate to technology and the delivery of technology services.

The '*Risk Owner*' was derived from the risk frameworks of each bank and from an industry perspective. From an APRA perspective all the risk components are owned by the bank's Board. Within each bank the ownership is delegated to business units to manage. During the analysis of CBA's and WBC's annual reports the delegated risk owner within the bank was identified according to which section of the annual report the risk component was addressed.

The '*impact rating*' is usually established through group or individual interviews held as part of the risk assessment process. However, for this study the author has taken the components and performed searches on the documents via queries in QSR NVivo then reviewed the content to identify and assess if the component was viewed on the scale from very high to low risk, managed well or under review. As part of the assessment certain components were given a rating based on sources outside the bank such as newspaper articles. The measurement techniques used in this study are aligned with those used by KPMG (2014) and PwC (2014). KPMG and PwC are the firms that developed the WBC and CBA risk governance frameworks respectively.

The '*Probability Rating*' is derived by evaluating the risk component according to industry knowledge of the researcher and therefore could be viewed as subjective, but it is in line with how Gartner calculate probability ratings as reported in articles by Scardino et al. (2005) and Lee et al. (2012) on an integrated framework for outsourcing risk management. For this analysis the subjective probability rating was applied consistently so if an error in a rating has been applied then it will be consistent across the sample and should not skew the findings.

### The Research Sample

The sample of the two banks analysed in this study was selected in part because they provided sufficient data in the public domain to enable the analysis. The other banks from an initial investigation did not provide sufficient data to enable the analysis to produce the required results. It was also believed these two banks would provide a reasonable percentage of the banking sector to allow the research results to be used to provide an industry level projection. Table 1 summarises the population and sample breakdown based on the figures extracted from the Australian Trade Commission (2011) for this study.

Table 1. Breakdown of the Population and Sample Selected

| Market Segments | AUD$ Billion | AFSI Market Share | Percentage of all ADIs | Percentage of the 4 Major Banks |
|---|---|---|---|---|
| AFSI population | $4,900 | 100% | | |
| Banking population 56 ADIs | $2,724 | 56% | | |
| 4 Major Banks | $2,000 | 41% | | |
| **Sample 2 Banks: CBA & WBC** | **$1,160** | **24%** | **43%** | **58%** |

## DATA ANALYSIS

### Regulatory Governance and Risk Frameworks

APRA applies one risk framework to govern operational risk using the AMA documented in a prudential standard (APRA 2013). Both banks in the study sample are approved to use this to measure and manage operational risk (APRA 2013). No evidence was found from the analysis of APRA's data that indicated that APRA monitors the risks associated with the percentage of IT services offshore-outsourced by each bank or how many different IT sourcing models the banks use.

**CBA Data Analysis**

Firstly we extracted information relating to IT services and methods of delivery from the CBA annual reports. Table 2 summarises this data (CBA 2009; CBA 2010; CBA 2011; CBA 2012; CBA 2013).

Table 2. CBA IT Trend Analysis

| CBA | Method of Delivery | | | |
|---|---|---|---|---|
| **IT Services** | **Outsource** | **Offshore-Outsource** | **Offshore** | **In-House** |
| **Infrastructure Services** | | | | |
| Data Centre | ☑ | | | ☑ |
| Desktop | ☑ | | | |
| IT Service Desk | ☑ | | | ☑ |
| Networking | ☑ | | | |
| Mobility | ☑ | | | ☑ |
| **Application Services** | | | | |
| Application Development | ☑ | | | ☑ |
| Application Maintenance | ☑ | | | ☑ |
| Application Support | ☑ | | | ☑ |
| Application Testing | ☑ | | | ☑ |
| **Enterprise Services** | | | | |
| Architecture | | | | ☑ |
| Engineering | ☑ | | | ☑ |

The sourcing landscape as shown in Table 2 demonstrates that CBA uses a complex IT multi-sourcing model. CBA uses outsourcing to deliver the majority of IT infrastructure services. The mix of IT service delivery models becomes more complex in the application services area. CBA has retained most of its enterprise services in-house as this is key Intellectual Property (IP) for the bank's IT strategy. One strategy CBA has never wavered from since the 1990s is that it does not send Australian jobs offshore (Newman 2013; Tait 2012).

In its annual reports from 2009 to 2011 CBA published details on long term IT contracts with a material impact, and included the following statement: "*In December 2007, the Bank entered into separate agreements with each of Tata Consultancy Services Ltd, HCL Technologies Ltd and IBM Australia Ltd for the provision of application software related services. As part of entering into these contracts, the Bank terminated certain parts of the previous long term agreement with EDS (Australia) Pty Ltd relating to application software services. The remaining parts of the contract with EDS (Australia) Pty Ltd - related to mainframe, midrange, end user technology and cards-related services - continue until 2012.*" This statement indicates a move from a dedicated IT outsourcing service provider providing all IT services to an IT multi-vendor model with the capabilities for IT multi-sourcing. It is interesting to note that the IT contracts declaration section of the report was omitted without explanation from the 2012 and 2013 annual reports.

*CBA – View of Risk and Governance*

The two focus areas for the analysis were the risk framework and the governance framework and how these coexist. Analysing these two frameworks provides the ability to check their alignment with the APRA risk and governance frameworks (APRA 2013).

CBA's operational risk definition has remained unchanged during the analysis timeframe: "*Operational risk is defined as the risk of economic loss arising from inadequate or failed internal processes, people, systems, or from external events. It includes legal, regulatory, fraud, business continuity and technology risks* (CBA 2013). It can be seen from CBA's operational risk definition that its technology risk is included as part of the definition which is in line with APRA's definition.

CBA's Risk Management Framework provides a 'three line of defence' model that provides a clear line of accountability, responsibility and auditability from the business unit level to the Board through the CBA Governance framework. The CBA Board structure provides independent governance of the bank. The link between the Board and the executive of the company is the Chief Executive Officer (CEO) who sits as a member of the Board. The Board has several committees that oversee the running of the bank. The only committee that includes the entire Board is the risk committee. This clearly demonstrates the focus CBA places on risk management and governance of risk.

Table 3. CBA Risk Profile

| Component of Risk Management | Risk Owner | Impact Rating | Probability Rating |
|---|---|---|---|
| Governance and Risk Management | Board | Very High | Low |
| Skills and Knowledge Management | Delivery | Very High | Medium |
| Companies fit and Alignment | Commercial | High | Low |
| Quality Management | Commercial | Medium | Medium |
| Sovereign Risk / On-Going concern | Legal | Low | Low |
| Offshore Facilities (capacity for growth) | Commercial | Low | Low |
| Commercial | Commercial | Very High | Medium |
| Sustainability | Delivery | Low | High |
| Critical projects | Delivery | Very High | High |
| Data Leakage and Confidentiality | Commercial | Low | Low |
| Service Provider Mix | Commercial | High | Low |

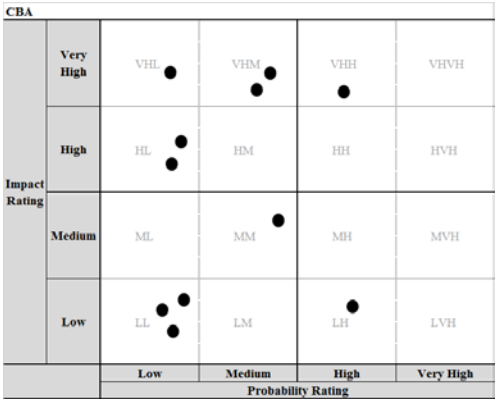



Figure 2. CBA Risk Map

Table 3 was populated from the results of the content analysis approach outlined in 'Research Approach' section detailed above.

Figure 2 shows the risk map based on the impact and probability values calculated by the researcher and shown in Table 3. It can be seen in Figure 2 that the impact of the risks has an even spread across three of the quadrants. This tells us that the impact to the bank for the majority of the risk would be fairly high but the probability of the risk being realised is fairly low. This infers that with the right level of management attention and monitoring, the risks are manageable.

**WBC Data Analysis**

In 2010, WBC made a decision to move Application, Development and Maintenance (ADM) services to a multi-vendor multi-sourcing delivery model. WBC selected four service providers to provide transformational ADM programs under the Strategic Improvement Priorities (SIP) programs. The SIP initiative aims to modernise all aspects of the bank.

Table 4. WBC IT Trend Analysis

| **WBC** | **Method of Delivery** | | | |
|---|---|---|---|---|
| **IT Services** | **Outsource** | **Offshore-Outsource** | **Offshore** | **In-House** |
| **Infrastructure Services** | | | | |
| Data Centre | ☑ | | | |
| Desktop | ☑ | | | |
| IT Service Desk | | ☑ | | ☑ |
| Networking | ☑ | | | |
| Mobility | ☑ | ☑ | | ☑ |
| **Application Services** | | | | |
| Application Development | | ☑ | | ☑ |
| Application Maintenance | | ☑ | | ☑ |
| Application Support | ☑ | ☑ | | ☑ |
| Application Testing | | ☑ | | ☑ |
| **Enterprise Services** | | | | |
| Architecture | | | | ☑ |
| Engineering | | | | ☑ |

The sourcing landscape as shown in Table 4 demonstrates that WBC has a complex mix of outsourcing, offshore-outsourcing and in-house delivery methods (IT multi-sourcing). It can be seen from Table 4 that the bank uses outsourcing to deliver the majority of IT infrastructure services. The application services area uses multiple delivery models. WBC has kept enterprise services in-house as this is regarded as key IP for the bank's IT strategy (WBC 2009; WBC 2010; WBC 2011; WBC 2012; WBC 2013).

From 2012 to 2013 WBC entered into agreements that influenced the composition of the IT service delivery model by introducing IT external service providers with offshore delivery capabilities thus creating an IT multi-vendor-multi-sourcing model:

1. In 2012, WBC signed two agreements each of five years duration with Tata Consultancy Services (TCS) to provide maintenance and development support within the information systems and customer self service areas of technology.
2. In 2012, WBC commenced two agreements with InfoSys Technologies to provide maintenance and development support within the testing, corporate systems, group customer master and customer assisted services areas of technology.
3. In 2013, WBC entered into an agreement with IBM Australia to provide project delivery resources for Integrated Migration and Transformation Program (IMTP) requirements.

*WBC – View of Risk and Governance*

The WBC operational risk definition has remained unchanged during the analysis timeframe. This definition is aligned with the definition provided by APRA (2013): "*The risk that arises from inadequate or failed internal processes, people and systems or from external events. This includes compliance risk, the risk of legal or regulatory sanction, and the financial or reputation loss arising from our failure to abide by the standards required of us as a financial services group*" (WBC 2013).

The following definition of Technology Risk was developed by WBC because of the changes introduced by the SIP initiatives: "*Our ability to develop and deliver products and services to our customers is dependent upon technology that requires periodic renewal. We are constantly managing technology projects including projects to consolidate duplicate technology platforms, simplify and enhance our technology and operations environment, improve productivity and provide for a better customer experience. This includes our current SIPs program. Failure to implement these projects effectively could result in cost overruns, a failure to achieve anticipated productivity, operational instability, reputational damage or operating technology that could place us at a competitive disadvantage and may adversely affect our results of operations.*" (WBC 2011). This definition enabled WBC to measure technology risk as a separate track outside operational risk. APRA embeds technology risk as part of operational risk.

To summarise, WBC's risk management framework and corporate governance model provide comprehensive management and governance of risk within the bank. The WBC Risk Defence Model drives risk appetite, policies and standards from top down. WBC then uses the three lines of defence to report and escalate from the bottom up similar to that used in CBA. As with CBA the non-executive leadership (the Board) and the executive leadership are kept separate to ensure that the day to day management of the bank does not interfere with the governance function of the bank. The conduit between the Board and the executive leadership is the CEO who is a member of the Board and heads the executive leadership team. The Board delegates responsibility to committees to provide focus on specific areas of the bank. The Board committees are made up of members of the Executive Board who provide subject matter expertise to the specific areas. Unlike CBA's risk committee which includes all of its Executive Board, WBC's risk committee includes all the Executive Board members *except* for the CEO. WBC has an additional committee that reports to the Board: the technology committee. The technology committee is chaired by a non-executive director from the Board and is the only committee that includes the CEO.

Table 5 was populated from the results of the content analysis approach outlined in 'Research Approach' section detailed above. Figure 3 shows the risk map based on the impact and probability values calculated in Table 5.

Table 5. WBC Risk Profile

| Component of Risk Management | Risk Owner | Impact Rating | Probability Rating |
|---|---|---|---|
| Governance and Risk Management | Board | Very High | Low |
| Skills and Knowledge Management | Delivery | Very High | High |
| Companies fit and Alignment | Commercial | Medium | Low |
| Quality Management | Commercial | Very High | Medium |
| Sovereign Risk / On-Going concern | Legal | Very High | Low |
| Offshore facilities (capacity for growth) | Commercial | Very High | Low |
| Commercial | Commercial | Very High | Medium |
| Sustainability | Delivery | Medium | High |
| Critical projects | Delivery | Very High | High |
| Data Leakage and Confidentiality | Commercial | Medium | Low |
| Service Provider Mix | Commercial | Very High | Medium |

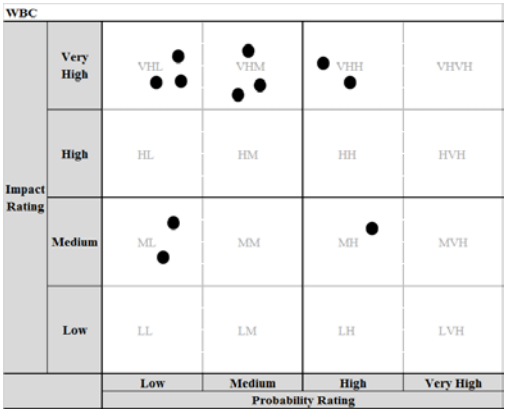



Figure 3. WBC Risk Map

It can be seen in Figure 3 that the impact of the risks identified in Table 5 are predominately in the top left and right quadrants of the map. This tells us that the impact on the bank for the majority of the risks would be

extremely high but the probability of the risk being realised for the majority of the risks is fairly low. This pattern indicates the bank needs to manage its risk profile very closely. WBC needs to apply a high level of focus at senior management level and executive attention and monitoring in order to control the risks. The need for board level visibility could explain why WBC instigated a technology committee reporting directly to the Board. This committee would provide the right level of focus on any potential impacts of the SIP initiatives and the changes in the IT sourcing strategy.

## DISCUSSION

### CBA IT Sourcing Strategy

The analysis of CBA shows that unlike WBC it does not have a technology committee that reports at the Board level, even though CBA is going through a major IT transformation and modernisation program similar to WBC.

Although the leadership of CBA states they do not offshore bank jobs, from the evidence collected and presented in the data analysis section, CBA certainly does have the capability to use its current IT service providers' offshore centres to obtain IT services without impacting on current CBA jobs. Up until and including the 2011 annual report CBA published a list of new material technology contracts, similar to WBC's disclosure. *In the 2012 and 2013 CBA annual reports this information was omitted*, CBA offered no explanation for this modification.

### WBC IT Sourcing Strategy

The data presented in the Data Analysis section demonstrates that WBC has a complex IT multi-sourcing model. WBC has a robust risk management and governance model that includes the business unit level all the way to Board level. This is in line with the APRA requirements and the analysis did not reveal any gaps between the APRA requirements as detailed in the APRA standard (APRA 2013) and the implemented model as documented in the Annual Report (WBC 2009) and each subsequent annual report in the sample.

On the surface it appears that WBC, from a regulatory perspective, has a sound foundation when managing its operational risk. During the analysis of the WBC reports a few questions were raised that need to be addressed. Why is the CEO not included on the WBC risk committee? The analysis of CBA shows its CEO is a member of the risk committee, the analysis did not provide any reason for this. Why does WBC include contractors in their FTE staff total? This is not the norm as FTEs form the basis of the budget reporting on permanent staff and these staff incur corporate overheads such as superannuation, long service leave, annual leave and sick leave. WBC has set up a technology committee that reports directly to the Board. The evidence shows this was done to help manage the risk associated with the SIP programs. If WBC views the risk associated with the changes introduced by the transformation and modernisation SIP program as needing visibility at Board level then why does APRA not require formal reporting of these transformation and modernisation risks?

### Prudential and Operational Risk Governance

APRA has provided a risk framework, guidelines and a method to assess risk (APRA 2013) and from the data analysis it is clear that both banks in the sample adhere to this standard. APRA developed APS 115 based on alignment to the Basel Committee accord, white papers and guidelines (Basel Committee on Banking Supervision 2004; Basel Committee on Banking Supervision 2005; Basel Committee on Banking Supervision 2011a; Basel Committee on Banking Supervision 2011b). This research has found the banks adhere to the directives published by APRA in the risk prudential standard APS 115.

Where there may be a gap is in the identification and treatment of risks associated with IT transformation programs and multi-sourcing of IT services. Are the current operational risk framework and guidelines sufficient to provide enough proactive protection across the AFSI? Another gap uncovered in the data analysis was that while WBC has a clear definition of technology risk, no definition of technology risk could be found in the APRA prudential standards. APRA does not appear to provide clear guidance on technology risk or the risks associated with multi-sourcing IT services. APRA has published two prudential standards that combined attempts to address the IT outsourcing strategy undertaken by the banks (APRA 2005; APRA 2006). One could argue that these standards provide sufficient protection because they address outsourcing and business continuity planning. What seems to be missing in APS 231 and APS 232 is that they do not address the risk associated with the complexity of combining outsourcing, offshoring and offshore-outsourcing to deliver IT services.

## CONCLUSIONS AND IMPLICATIONS

APRA's prudential standard on risk and provision of capital adequacy using AMA (APRA 2013) appears to provide a sound risk framework to manage operational risk in a consistent and stable environment. But from the findings of this study neither bank would appear to have a consistent or stable environment especially from a

technology perspective. The current prudential standards use capital adequacy to mitigate the risk e.g. enough funds available to address the risk if it is realised. In the technology environment, financial resources may not be the ideal remedy to mitigate risk. The impact of a failure is immediate and time is the enemy as the longer a problem exists the more likely it will undermine consumer confidence in the banking system. So perhaps a proactive risk management framework is needed rather than the reactive risk framework currently used by APRA in its prudential standards.

In terms of the research questions, the results show a complex IT delivery model exists within each bank and each has a different risk complexity matrix (RQ1). Both CBA and WBC have one risk framework that governs all risk areas. It is based on the APRA risk framework guidelines published in APS 115 (RQ2). There is a need for APRA to provide a proactive risk management framework to mitigate risks associated with a failure in an IT system, process or people when an organisation sources the delivery of its IT services under more than one delivery model (RQ3). Future research is needed to explore the cumulative impact of risks associated with the IT multi-sourcing strategies employed by the 'big four' Australian banks as part of their modernisation initiatives.

The limitation in this study is recognised in that the analysis of the two banks and governing bodies relied on reports made available in the public domain. However it should be recognised the majority of the bank reports are reliable sources of information as they are certified either by officers of the banks, public auditors or government regulators. The reports from the governing bodies are all from government organisations that are monitored and accountable to the government and public. In this study the author was unable to confirm the research findings through the use of empirical evidence without carrying out interviews with the decision makers and risk component owners from the banks.

From these findings, we recommend APRA considers the development and management of a more comprehensive risk model that acknowledges and provides clear guidance on how to manage the risks associated with IT sourcing and in particular IT offshore-outsourcing. There is a need to provide a proactive risk management framework to mitigate risks associated with a failure in an IT system, process or people when an organisation sources the delivery of its IT services from more than one delivery model. Hence there is a need to provide a risk weighting that reflects whether the IT services are managed in-house, outsourced domestically or offshore-outsourced. Such a risk weighting matrix would indicate the complexity of the mix of IT service delivery models within each bank. The risk framework also needs to address the volume, complexity and cumulative effect of the banks' multi-sourcing models on the industry and economic risk profile.

In conclusion, the aim of this paper has been achieved: we have demonstrated the complexity and risk of the current IT delivery environment within two large Australian banks. We have made a contribution to address the gap in research regarding the critically important issues surrounding risk management and governance within the banking sector of the AFSI.

## REFERENCES

Alexander, K. 2006. "Corporate Governance and Banks: The Role of Regulation in Reducing the Principal-Agent Problem," *Journal of Banking Regulation* (7:1/2), pp. 17-40.

APRA. 2005. "Prudential Standard Aps-232," in: *Business Continuity Management*, APRA (ed.). Australia: APRA, p. 8.

APRA. 2006. "Prudential Standard Aps-231," in: *Outsourcing*. Australia: APRA, p. 7.

APRA. 2013. "Prudential Standard Aps 115 " in: *Capital Adequacy: Advanced Measurement Approaches to Operational Risk*, APRA (ed.). Australia: APRA, p. 30.

Australian Government. 1959. "Banking Act 1959 Act No. 6 of 1959 as Amended," C. Attorney-General's Department (ed.). Canberra: Office of Legislative Drafting and Publishing, p. 173.

Australian Trade Commission. 2011. "Australia's Banking Industry," Austrade (ed.). Australia: Australian Government, p. 76.

Basel Committee on Banking Supervision. 2004. "International Convergence of Capital Measurement and Capital Standards - a Revised Framework," in: *The Bank for International Settlements*. Basel, Switzerland: Basel Committee Publications, p. 251.

Basel Committee on Banking Supervision. 2005. "Outsourcing in Financial Services," in: *The Joint Forum*. Basel, Switzerland: Basel Committee Publications, p. 28.

Basel Committee on Banking Supervision. 2011a. "Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches," in: *Basel Committee on Banking Supervision*. Basel, Switzerland: Basel Committee Publications, p. 63.

Basel Committee on Banking Supervision. 2011b. "Principles for the Sound Management of Operational Risk," in: *Basel Committee on Banking Supervision*. Basel, Switzerland: Basel Committee Publications, p. 27.

CBA. 2009. "Annual Report 2009," Australia, p. 234.

CBA. 2010. "Annual Report 2010," Australia, p. 242.

CBA. 2011. "Annual Report 2011," Australia, p. 241.

CBA. 2012. "Annual Report 2012," Australia, p. 230.

CBA. 2013. "Annual Report 2013," Australia, p. 197.

Eisenhardt, K.M. 1989. "Agency Theory: An Assessment and Review," *Academy of Management Review* (14:1), pp. 57-74.

Guthrie, J., Petty, R., Yongvanich, K., and Ricceri, F. 2004. "Using Content Analysis as a Research Method to Inquire into Intellectual Capital Reporting," *Journal of Intellectual Capital* (5:2), pp. 282-293.

Kirkegaard, J.F. 2008. "Offshoring, Outsourcing and Production Relocations — Labor Market Effects in the OECD and Developing Asia," *The Singapore Economic Review* (53:3), pp. 371-418.

KPMG. 2014. "Managing Risk and Complexity " Retrieved 18/05/2014, 2014, from http://www.kpmg.com/au/en/topics/managing-risk-complexity/Pages/default.aspx

Krippendorff, K. 2013. *Content Analysis an Introduction to Its Methodology*, (Third ed.). United States of America: SAGE Publications, Inc.

Lee, C.K.M., Yeung, Y.C., and Hong, Z. 2012. "An Integrated Framework for Outsourcing Risk Management," *Industrial Management & Database Systems* (112:4), pp. 541-558.

Newman, R. 2013. "Commonwealth Banks." Retrieved 18/03/2014, 2014, from http://finance.ninemsn.com.au/newsbusiness/motley/8704858/commonwealth-will-not-offshore-jobs

PwC. 2014. "Financial Services Regulation." Retrieved 18/05/2014, 2014, from http://www.pwc.com.au/industry/financial-services-regulation/index.htm

Scardino, L., Anderson, D.S., Brown, R.H., Da Rold, C., Dreyfuss, C., Karamouzis, F., Lovelock, J.-D., Maurer, W., Moore, C., and Young, A. 2005. "Gartner on Outsourcing," in: *Gartner on Outsourcing, 2005*. Gartner, pp. 1-42.

Stemler, S. 2001. "An Overview of Content Analysis," *Practical assessment, research & evaluation* (7:17).

Strijbos, J.-W., Martens, R.L., Prins, F.J., and Jochems, W.M.G. 2006. "Content Analysis: What Are They Talking About?," *Computer & Education* (46:1), pp. 29-48.

Tait, V. 2012. "Cba Rejects Need to Send Jobs Offshore." Retrieved 18/03/2014, 2014, from http://www.morningstar.com.au/stocks/article/rejects-need-to-send-jobs-offshore/4702

Terry, C. 2009. "The New Basel Capital Accord: A Major Advance at a Turbulent Time," *Agenda: A Journal of Policy Analysis and Reform* (16:1), 2009, pp. 25-43.

WBC. 2009. "2009 Annual Report," Westpac Banking Corporation, Australia, p. 300.

WBC. 2010. "2010 Annual Report," Westpac Banking Corporation, Australia, p. 316.

WBC. 2011. "2011 Annual Report," Westpac Banking Corporation, Australia, p. 312.

WBC. 2012. "2012 Annual Report," Westpac Banking Corporation, Australia, p. 308.

WBC. 2013. "2013 Annual Report," Westpac Banking Corporation, Australia, p. 316.

## INTELLECTUAL PROPERTY