University of Southern Queensland

Prudential Regulatory Governance of the Risks Associated with IT Multi-Sourcing Strategies within the Australian Banking Sector

A Dissertation submitted by Brian Strong for the award of
Master of Business Research
2014

Abstract

Concerns about the adequacy of the Australian Prudential Regulatory Authority (APRA) prudential standards to govern the risks associated with the Australian banks' multi-sourcing IT service delivery strategies provided the motivation for conducting this study. Three research questions were developed to investigate prudential risk management in the banking sector of the Australian Financial Services Industry (AFSI). RQ1: Do the banks employ complex multi-sourcing solutions driven by business unit demands to deliver their IT services? RQ2: What are the risk and governance model/s used by the banks to manage risks associated with their IT services multi-sourcing strategy? RQ3: Is the AFSI IT operational risk exposure adequately covered by the current APRA risk framework and prudential standards?

The two largest Australian banks, Commonwealth Bank of Australia (CBA) and Westpac Banking Corporation (WBC) referred to as the 'banks' in this research are selected as the sample. CBA and WBC are the first and second largest banks when measured by capitalisation within the banking sector of the AFSI and represent 43 percent sample of the capitalisation value of the AFSI. Although profitable, the banks are under pressure from the market to reduce their cost-to-revenue ratio. One of the main strategies the banks employ to reduce IT costs is the outsourcing the delivery of IT services.

Over the past five years a trend has evolved with the banks using offshore-outsourcing to deliver IT services and gain further IT savings. However little empirical research has investigated what impact this trend has had on the risk profile of the banks and the Australian banking sector as a whole. This research identified and investigated the different IT services delivery models adopted by the banks by analysing on the relevant literature and documentation available in the public domain in relation to the AFSI. The findings of this research developed a picture of the IT delivery landscape within the banking sector of the AFSI. Findings of this research also demonstrates the complexity of the banks operational environment which can be attributed to the banks' introduction of their IT multi-sourcing strategies. Finally the findings of this research raise some questions about whether the risks associated with an increasing reliance on IT multi-sourcing to deliver IT services is adequately managed by Australian banking sector and the regulatory framework of APRA.

Keywords

IT outsourcing, IT offshore-outsourcing, risk, governance, Australian banks, decision theories, Australian Prudential Regulatory Authority, BASEL, IT service delivery, multi-sourcing.

Certification of Dissertation

I hereby declare that this submission is my own work and to the best of my knowledge it contains no material previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any other degree or diploma at University of Southern Queensland or any other educational institution, except where due acknowledgement is made in the dissertation. Any contribution made to the research by others, with whom I have worked at University of Southern Queensland or elsewhere, is explicitly acknowledged in the dissertation.

I also declare that the intellectual content of this dissertation is the product of my own work, except to the extent that assistance from others in the project's design and conception or in style, presentation and linguistic expression is acknowledged.

During the course of the project, a research-in-progress paper was accepted for presentation as a poster at AMCIS and published in the conference proceedings: Strong, B, Cater-Steel, A & Lane, M 2014 'Prudential Risk Management of IT Sourcing Strategies: A Case Study of an Australian Bank', *20th Americas Conference on Information Systems (AMCIS)*, Savannah, Georgia, USA.

_____ / /2014

Brian Strong

Endorsed by:

_____ / /2014

Professor Aileen Cater-Steel, Principal Supervisor

_____ / /2014

Dr. Michael Lane, Associate Supervisor

Acknowledgement

My initial interest in this research topic was inspired by my experience in managing large IT outsourcing accounts for the largest global outsourcing providers. During my time delivering IT outsourcing solutions I saw 'the good, the bad and the ugly' from both the service provider as well as the customer's side. Followed my twenty plus year career with service providers I moved into the customer side, some have referred to this as a 'poacher turned gamekeeper'. I specialised in developing sourcing strategies, vendor selection processes and governance models for large companies. During this time I developed a multi-sourcing approach that involved mixing outsourcing and offshoring solutions depending on the services being purchased. Again during this time I saw 'the good, the bad and the ugly', and more importantly to this research, the downright dangerous approaches to solving business challenges.

Firstly I would like to provide my thanks to Professor Aileen Cater-Steel who from our first meeting in Sydney in November 2012 has always provided excellent counsel to a novice researcher. Aileen has that unique ability to guide a person so they deliver the best consistently. Without her support and mentorship I probably wouldn't have even started on this path. Next I would like to extend my thanks to my associated supervisor Dr Michael Lane who provided the guidance I needed (not always wanted) to produce quality output with the most relevant materials that provided the needed foundation to my work. Finally I would like to thank Libby Collett who has great enthusiasm, but I am sure was bored while she proof read my dissertation.

To the most important people in my personal life, to my wife Trish for her support and encouragement during this journey. On the days when I wanted to pack it all in and return to my previous life she provided the encouragement I needed to keep going. To my daughter Ceara who although didn't have to suffer my daily ups and downs did provide me with phone and text support. Finally I need to thanks those that provided informal mentoring support, David, Deirdre and Sharon. They probably don't realise the support they provided but I thank them for their support.

Brian Strong

University of Southern Queensland

TABLE OF CONTENTS

SECTIONS

List of Figures

List of Tables

Abbreviations

ADI	Authorised Deposit-taking Institutions, defined in the Banking Act 1959
ADM	Application Development and Maintenance
AFSI	Australian Financial Service Industry
AMA	Advanced Measurement approach used to calculate the capital allocation for risk under the APRA and Basel risk framework
ANZ	Australia and New Zealand Banking Group Limited (http://www.anz.com.au/personal/)
APRA	Australian Prudential Regulatory Authority (http://www.apra.gov.au/Pages/default.aspx)
APS	Australian Prudential Standard, standard used by APRA to govern all ADIs
APS 115	Standard used by APRA to provide the framework and requirements for ADIs to meet the regulatory capital requirements when using Advanced Measurement Approaches (AMA) to operational risk management
APS 231	Standard used by APRA to govern who use or intend to use outsourcing as a mean of delivering services from a service provider to the ADI
APS 232	Standard used by APRA to govern ADI ability to meet its business continuity management function, also used in conjunction with APS 231 outsourcing
ASIC	Australian Securities and Investment Commission (http://www.asic.gov.au/)
BCBS	Basel Committee on Banking Supervision
BCM	Business Continuity Management
BASEL	The committee responsible banking supervision and is part of the Bank of International Settlements based in Basel Switzerland
BASEL I, BASEL II and BASEL III	Revisions of the accords developed by the BCBS to provide bank supervisory bodies with a framework to manage risk and capital liquidity of individual banks
Captive	This is an industry term referring to where a customer sets up a centre in an offshore location and retains full ownership and utilises the customer brand
CBA	Commonwealth Bank of Australia (http://www.commbank.com.au/)
CFR	Council of Financial Regulators (http://www.cfr.gov.au/)
CTB	Change The Bank, commonly used term within the banking industry, defined as application and bespoke IT solution used to provide innovation and transformational solution to the banks
GDP	Gross Domestic Product
GFC	Global Financial Crisis
IP	Intellectual Property
KBT or KBV	Knowledge-based theory or view of the firm – Theory

KPI	Key Performance Indicators
MSA	Master Service Agreement, a legal and commercial group of instruments that defines how the engagement between the customer and service provider are governed and managed
NAB	National Australia Bank Limited (http://www.nab.com.au/)
RBA	Reserve Bank of Australia (http://www.rba.gov.au/)
RBT or RBV	The resource-based view of the firm – Theory
RTB	Run The Bank, commonly used term within the banking industry, defined as infrastructure, core systems and support functions that are required to keep the bank running.
SIP	Strategic Improvement Priority
SLA	Service Level Agreement
SoW	Statement of Work
TCE	Transaction cost economics – Theory
UNCTAD	United Nations Conference on Trade and Development
WBC	Westpac Banking Corporation (http://www.westpac.com.au/)

Chapter 1 Introduction

This Chapter lays the foundation for the study and also introduces the concepts used in the remainder of this dissertation. Figure 1.1 provides an overview of this chapter, and a similar diagram is used in each chapter forming the first part of the introduction section of each chapter.

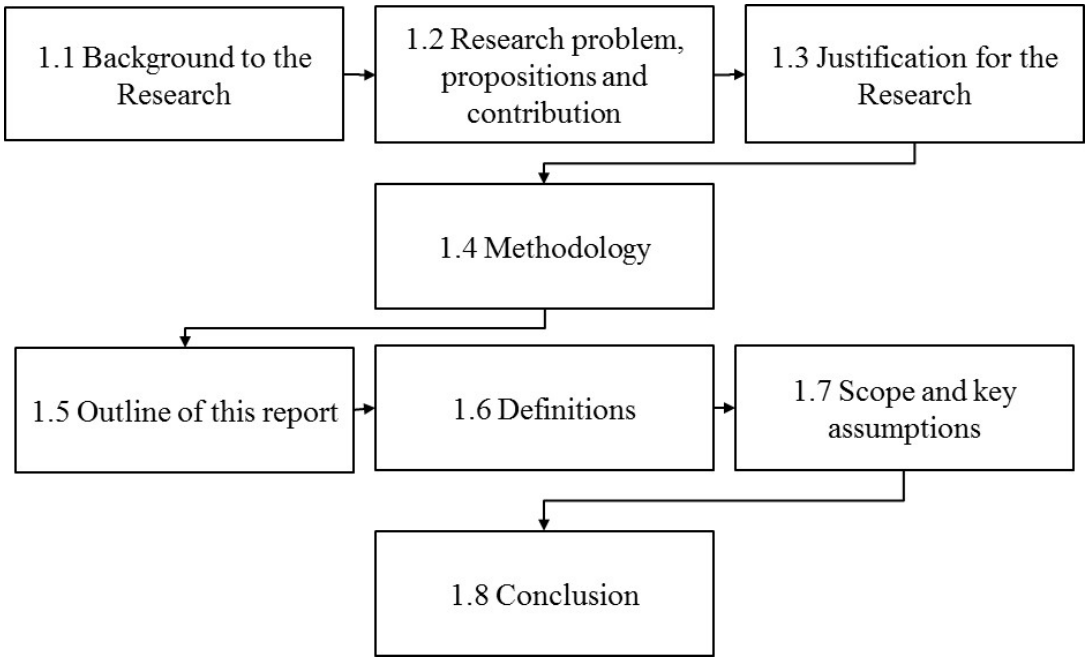


Figure 1.1 – Chapter 1 Structure

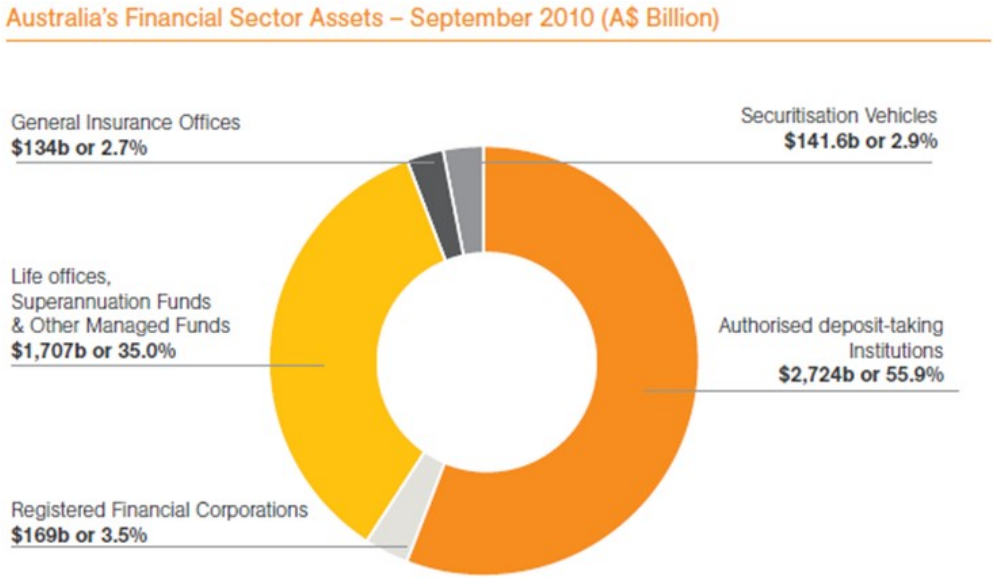
From Figure 1.1 it can be seen there are eight sections in Chapter 1, which forms the introductory chapter of this dissertation. Section 1.1 provides the background and reasons for embarking on the study. Section 1.2 provides an overview of the problem, propositions and contribution of the study. Section 1.3 provides the introduction to the significance of this study and how it contributes to the overall knowledge base of the academic community. Section 1.4 outlines the methods used for collecting and analysing the data to support the study. Sections 1.5, 1.6 and 1.7 provide an overview of this dissertation and the key assumptions and definitions used in this document. Finally, the conclusion section summarises this chapter and also provides a link to the next chapter of the dissertation.

1.1 Background to the Research

This study is inspired by the researcher's experience in building and managing some of the largest IT outsourcing accounts for global outsourcing service providers. This study provides a background of each of the IT business units of the banks' and the IT service delivery models employed by each IT business unit. The study then investigates how decisions made by the bank's IT business units could have an influence on the operational risk profile of the banking industry within Australia. Finally the study analyses the industry level risk management framework APRA (2013a) and its efficiency in managing any potential risk exposure caused by the decisions made by the banks in how they deliver IT services that support their business.

1.1.1 Composition of the AFSI

Figure 1.2 shows the composition of the Australian Financial Services Industry (AFSI) as at February 2011.



Source: Australian Trade Commission, *Australia's Banking Industry*, 2011, P. 6

Figure 1.2 – Composition of the AFSI

The AFSI manages AUD$4,900 billion worth of assets which equates to 240 percent of Australia's nominal gross domestic production (GDP). The banking sector within the AFSI is comprised of 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 and contribute 10 percent (AUD$135 billion) of Australia's annual output.

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). The four major banks are Westpac Banking Corporation (WBC), Commonwealth Bank of Australia (CBA), National Australia Bank Limited (NAB) and Australian and New Zealand Banking Group Limited (ANZ). The study sample is restricted to two of the four major Australian banks or ADIs as a Masters Research timeline would not permit investigation into all 56 ADIs. Within the ADIs, which represent 55.9 percent of the AFSI, we have selected two of the four major banks as our sample for this study. The author has selected CBA and WBC for this study, as they are the first and second largest banks when ranked by capitalisation within the banking sector of the AFSI.

It also should be highlighted that the banks trade in the other four slices of the pie in Figure 1.2, but the banking licence only applies to the ADI component of the functions they perform. Finally, part of the rationale in selecting the sample of CBA and WBC as two of the four major banks in Australia is that the prudential standards that form the regulatory foundation of this study only apply to ADIs that are licensed to trade as a bank in Australia (Australian Trade Commission 2011). Hereafter in this dissertation these two banks are referred to as "the banks" and form the scope of this Masters Research study within the banking sector of the AFSI.

The sample for the research project represents 43 percent (AUD$1,160 billion) of the market value of assets managed under AFSI. Table 1.1 summarises the sample breakdown based on the figures extracted from the Australian Trade Commission (2011).

Table 1.1 – Research Sample

Market Segments	AUD$ Billions	AFSI Market Share	Notes
ADI	2,724	100%	Total bank population
WBC & CBC	1,160	43%	The sample

1.1.2 APRA Governance of the AFSI

The AFSI is a highly regulated industry governed by the Australian Prudential Regulatory Authority (APRA). APRA is a statutory authority established in 1998 and is legislated by the Banking Act 1959 (Australian Government 1959) to perform the function of prudential supervision to the financial institutions within the AFSI and also ensure financial system stability within the AFSI and the Australia economy is maintained. APRA is funded largely by the industries that it supervises. Further details of its vision, mission and strategy are provided in its charter in APRA (2010). APRA utilises prudential standards as the regulatory instruments to manage all aspects of the banking business that have the potential to impact customers and/or the Australian economy. The importance of tight government prudential regulation was demonstrated at the time of the Global Financial Crisis (GFC) as banking sector in Australia proved to be one of the few banking sectors protected from this crisis.

Although profitable, the banks are under pressure from the market, media and major shareholders to reduce their cost to revenue ratio. One of the main cost reduction strategies the banks employ is to reduce IT costs. This, in part, has been achieved through outsourcing their IT services. Subsequently a trend has evolved over the last five years in the banking sector of the AFSI to adopt an IT offshore-outsourcing services model. This move achieved further cost saving and access to a larger skilled resource pool. While visiting one of Westpac's operations in India, Mrs Kelly, CEO of WBC, defended the practice by saying it had allowed the bank to work with "world-class" companies such as IBM and had given WBC access to highly skilled workers: "*The strategy is not about cost arbitrage, the strategy is about skill enhancement*" (Yeates 2013). Each of the bank's IT business units adopted a different evolutionary path to provide IT services in their organisation. From information gathered from the banks' annual reports it appears that both banks are following a multi-sourcing IT services strategy to manage cost, quality and delivery of IT services (CBA 2011b; WBC 2013).

1.1.3 Regulatory Governance of Outsourcing

Regulatory governance of outsourcing is managed under the Council of Financial Regulators (CFR) framework. The CFR is comprised of APRA (see APRA 2010), the Australian Securities and Investment Commission (ASIC), the Reserve Bank of Australia (RBA) and the Treasury department of the Australian government. APRA is legislated by the Banking Act 1959 (Australian Government 1959) to perform a prudential risk governance role within the AFSI and to enforce adherence to the Australian Prudential Standards (APS).

APRA employs two prudential standards to manage IT risk associated with outsourcing the IT component of the banking services delivered to their customers. The first prudential standard APS 232 (APRA 2005) details the requirements for business continuity management (BCM) services within the banks. The second prudential standard - APS 231 (APRA 2006) - provides the requirements for managing risk associated with the banks' outsourcing activities. The third prudential standard - APS 115 (APRA 2013a) - is used by APRA to govern operational risks.

This research evaluates the banks' IT multi-sourcing service delivery models and associated risks. This evaluation ascertains if the prudential standards (APRA 2005, 2006) and the APRA risk management framework (APRA 2013a) provide sufficient proactive risk management to govern the cumulative risks introduced by the banks' IT multi-sourcing strategies. The study, informed by the literature, reviews the theories underpinning the decision-making processes that have a bearing on the banks' choices of IT sourcing delivery models. The researcher has identified the governance model/s and risk framework/s used to manage the different IT sourcing delivery models and risks associated with them. These three lenses (risk frameworks, governance models and decision-making theories) provide a picture of the banks' IT service delivery model in terms of IT sourcing.

Next the researcher has used the banks' IT service delivery models as a foundation to review and determine if APRA's governance of the banks' IT services sourcing strategies were adequately covered. Finally, the researcher evaluated public domain data on APRA's governance and the banks' IT services sourcing strategies and has projected that industry level risks were not addressed under the current APRA prudential regulations for outsourcing and operational risk management (APRA 2005, 2006, 2013a).

1.2 Research Problem and Propositions

1.2.1 Research Problem

Concerns have been raised about the adequacy of APRA's guidelines to manage the banks' multi-sourcing IT service delivery strategies (Bennet 2012; Durie & Gluyas 2009; Flinders 2014). Furthermore, given the multi-sourcing approach to IT service delivery by the banks, would there be a negative impact on the banking sector or even on the economic risk profile of the Australian economy if a catastrophic event were to occur?

1.2.2 Research Propositions

The author has used theories on decision making such as agency theory (Eisenhardt 1989), transactional cost theory (Coase 1998) and resource based theory (Barney, Wright & Ketchen 2001) to develop a greater understanding of the rationale behind the banks using different IT sourcing methods. In Chapter 2 this study has reviewed the management and governance of risks associated with the different IT sourcing delivery models. The conceptual model for this research was developed and is provided in Figure 1.3. The model comprises three levels of governance, starting from the left side of the model presented in Figure 1.3. The lowest level of risk governance and management is performed at the business unit level where the selection of an IT sourcing delivery model is made for a particular IT service function. The next level is the bank governance at Board level that has responsibility for setting the risk thresholds and ensuring adherence to the risk framework. The final level is the industry level risk governance function that is performed by APRA.

The conceptual model demonstrates the relationship between the decisions to select a specific IT sourcing delivery model. The governance framework used to manage the risks associated with the IT sourcing delivery model.

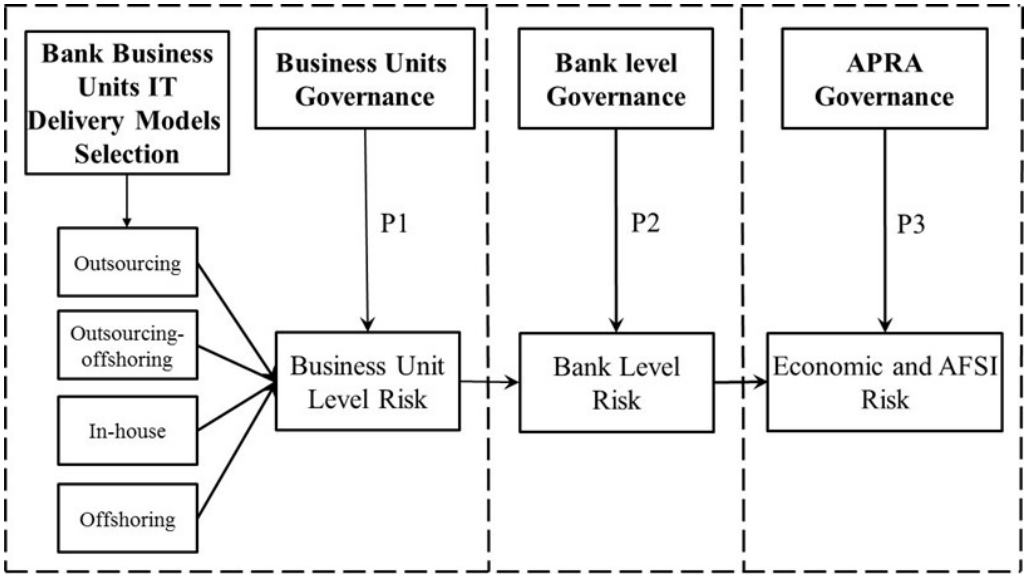


Figure 1.3 – Conceptual Model

The following propositions underpin the conceptual model:

P1. Each of the banks' business units select sourcing models based on their individual needs and they govern and manage their own operation risk.

P2. Each bank uses a single risk framework based on the APRA (2013a) guidelines for the governance and management of operational risk across all of the bank's business units.

P3. APRA's risk framework does not govern the cumulative industry operational risk associated with the individual banks' business units' selection of an IT sourcing model.

From a preliminary review, neither bank chosen in the sample has established an offshoring capability to deliver IT services. Therefore the focus of this study is to review the mix of outsourcing, offshore-outsourcing and in-house IT delivery models to determine and evaluate the risk profile of each bank and the industry level risk profile.

1.3 Justification for the Research

This study is based on a five year longitudinal case study of two banks in the AFSI and the risks associated with IT multi-sourcing. It also analyses whether or not the current risk and governance frameworks published by APRA are used in each bank, and 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.

1.3.1 Expected Contribution

The author has developed an IT sourcing landscape for each bank and a consolidated banking sector IT sourcing landscape. These are then used to develop the risk profiles and risk maps for each bank and the banking sector. This provides visibility of the different IT sourcing models and the risk exposure the banks need to manage. The industry level risk profile and map shows the cumulative effect of the

banks' IT sourcing strategies that APRA need to govern in order to manage the risk exposure to the banking industry and the Australian economy.

The key contribution of the analysis is to demonstrate whether or not the current APRA prudential standards and risk framework is sufficient to manage the economic risk associated with the operational risks introduced by the banks' current multi-sourcing strategies to delivery IT services.

The analysis in this study highlights how the current AFSI governance and risk management models could be enhanced based on international comparative research of the finance industry (Alexander 2006).

1.3.2 Expected Significance

As part of the banks' IT multi-sourcing strategy there is a risk that offshore-outsourcing of AFSI IT '*thought leadership*' or '*intellectual property*' could result in a gap in IT skills capability. If the offshore-outsourcing economies fail to remain economically viable the banks' IT multi-sourcing strategy could fail and it would take generations to fill the banking IT skills capability gap with local resources (Lane & Van der Vyver 2006). A good example of this issue is the Republic of Ireland. During the GFC the Irish economy collapsed due partly to lax banking prudential regulations (Connor & O'Kelly 2012) which resulted in companies such as Dell relocating services provided from Limerick in Ireland to Lodz in Poland in order to remain cost competitive (Collins & Grimes 2011). News reports indicate an upward trend within the AFSI to shift the provision and management of IT services to India. Could there be negative ramifications to the Australian economy if India became too expensive due to their cost of living increasing substantially (Agrawal, Pandit & Menon 2012)? This research project contributes to the regulatory governance and risk management literature with a specific focus on the banking sector's IT multi-sourcing strategies within the banking sector of the AFSI.

1.4 Methodology

1.4.1 Research Approach

This study is based on a five year longitudinal case study of two banks. This research drew upon information sourced from academic publications, information in the public domain made available by the banks, service providers, consultancy companies, APRA, BCBS and other Australian government agencies. Searches of the banks' web sites were conducted to identify data relating to the banks' IT services sourcing landscape and risk frameworks and governance models employed to manage IT services. A systematic search of the APRA, BCBS and Australian Bureau of Statistics (ABS) web sites was undertaken to ascertain information available on risk frameworks and governance models defined and implemented within the AFSI. Academic databases were searched to identify journal articles relating to the financial industry regulators' governance of IT services, IT services sourcing models and theories used to help understand the decisions to select certain types of sourcing models to deliver IT Services.

A search of IT service providers, media publications and consultancy company websites was used to supplement and verify the information gathered from the banks' and government websites specific to the AFSI.

1.4.2 Data Collection Approach

Firstly, to undertake the analysis of the banks' IT multi-sourcing activities, the author has extracted the five annual reports from 2009 to 2013. In the next step, the

data available on the APRA website was extracted to identify how APRA treats the three sourcing delivery models under the current prudential standards.
Output from the analysis of the information gathered from these two areas. - regarding the bank sample and APRA was used to build a picture of the exact nature of the scope and depth of the banks' IT sourcing strategies and APRA's governance activities in relation to the banks' IT sourcing strategies.

1.4.3 Output Development

Based on the artefacts presented in Chapter 4 the final presentation of the material that addresses the research problem, research propositions and overarching research questions are produced. All the findings are presented in a tabular and graphical format.

1.5 Scope and Key Assumptions

From an industry perspective the scope of this study is restricted to the two of the four major banks in Australia, specifically CBA and WBC. From the industry regulatory perspective, all information gathered is from APRA as it is the nominated body empowered by the RBA and government legislation to govern the finance industry within Australia. From a regulatory governance perspective guidelines and papers produced by BCBS that support or contributed to the APRA approach and prudential standards are included in the data collection and analysis. The study draws on industry documents created and published by the banks between the years 2009 to 2013 inclusive. The output from the data analysis completed on the banks and APRA documents was then used to develop an IT multi-sourcing model for each bank and a consolidated view that can be used in future studies as a foundation for industry projections on the effects of changes in the banks' IT sourcing strategies.

1.6 Definitions

The following definitions have been drawn from professional bodies, government agencies or respected academic journals. They are provided to assist the reader in understanding the meaning and context the terms used throughout this thesis.

IT Services: the Gartner definition of IT Services is used in this study: "*IT services refers to the application of business and technical expertise to enable organizations in the creation, management and optimization of or access to information and business processes. The IT services market can be segmented by the type of skills that are employed to deliver the service (design, build, run). There are also different categories of service: business process services, application services and infrastructure services. If these services are outsourced, they are referred to as business process outsourcing (BPO), applications outsourcing (AO) and infrastructure outsourcing*" (Gartner 2013).

External Service Provider: Gartner defines External Services Provider (ESP) as "*an enterprise that is a separate legal entity from the contracting company that provides services such as consulting, software development — including system integration and application service providers (ASPs) — and outsourcing. ESPs supplement the skills and resources of an in-house IS department*" (Stemler 2001).

In the context of this study, the term 'external service provider' refers to companies that provide outsourcing and or offshore-outsourcing IT services.

Outsourcing: There are many definitions of outsourcing, as clearly demonstrated by Dibbern et al. (2004) who provided an exhaustive literature review and definitions for 'outsourcing' and 'offshoring'. For the purpose of this study we

applied the definition provided by APRA in the prudential standard and implemented by banks intending or using outsourcing as a means of IT service delivery. The APRA definition in the prudential standard reads: "*Outsourcing involves an ADI entering into an agreement with another party (including a related body corporate) to perform, on a continuing basis, a business activity which currently is, or could be, undertaken by the ADI itself.*" (APRA 2006, p. 2).

Offshoring: There are various definition for offshoring. For this study the author has used the definition published by APRA as follows: "*the outsourcing by an ADI of a material business activity associated with its Australian business to a service provider (including a related body corporate) where the outsourced activity is to be conducted outside Australia.*" (APRA 2013c, p. 6). Another definition of offshoring is 'captive' offshoring. This model is where the company establishes its own delivery centre in an offshore location rather than buying the services from an external service provider from an offshore location.

Offshore-outsourcing: In the absence of a formal definition from a professional body, government agency or respected academic journal, the author has combined the definitions used by APRA for outsourcing and offshoring to form a relevant definition that fits the criteria for this study. The combined APRA definitions for offshoring and outsourcing reads as follows: '*Offshore-outsourcing involves an ADI entering into an agreement with another party (including a related body corporate) to perform, on a continuing basis, a business activity which currently is, or could be, undertaken by the ADI itself and where the material business activity associated with its Australian business to a service provider (including a related body corporate) where the outsourced activity is to be conducted outside Australia.'*

Multi-sourcing: Is where "*there is one outsourcing contract but multiple suppliers of services*" (Dibbern et al. 2004, p. 11). This allows the customer to manage multiple external suppliers under a single commercial arrangement.

Operational risk: For this project the author has used the definition APRA published as this is the definition the regulator and the banks should be using. APRA defines operational risk as "*the 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 risks*" (APRA 2013c, p. 6).

Legal Risk: APRA defines legal risk as "*Legal risk includes, but is not limited to, exposure to fines, penalties or punitive damages resulting from supervisory actions as well as ordinary damages in civil litigation, related legal costs and private settlements "* (APRA 2013c, p. 6).

Risk Management: In the fact sheet on AS/NZS ISO 31000:2009 Risk Management published by Comcover, an Australian Government department, risk is defined as "*the effect of uncertainty on objectives*", therefore risk management is the management of the uncertainty (Australian Government Comcover 2010, p. 1).

ADI: The APRA definition of an ADI "*refers to an authorised deposit-taking institution, meaning a body corporate authorised under section 9 of the Act, to carry on banking business in Australia (e.g. a bank, building society or credit union)*" (APRA 2013c, p. 2).

RTB: 'Run the bank' refers to the core banking systems, processes and people require to keep the bank running in '*business as usual*' fashion (Mestchian (2012).

CTB: 'Change the bank' refers to "*long-term (up to five years) strategic projects*" (Mestchian 2012) to change RTB systems, processes and people. Both CBA and WBC are going through major CTB programs to modernise the banks.

1.7 Outline of this Masters Dissertation

Figure 1.4 outlines the structure of the body of this dissertation and this is followed by a brief summary of the contribution of each chapter to the dissertation.

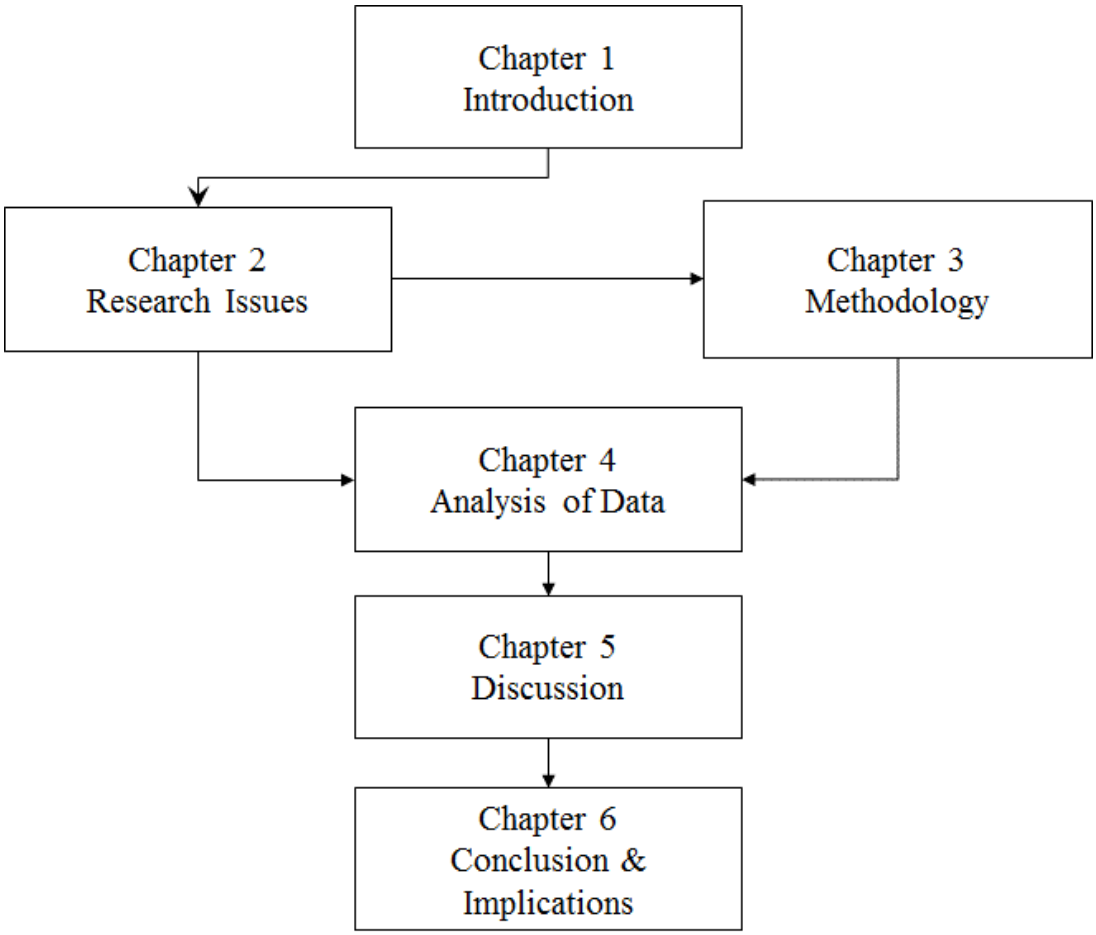


Figure 1.4 – Outline of the Dissertation Chapters

Chapter 1 '*Introduction*', provides the reader with a background to the scope of the study and introduces the stakeholders within the industry. It also outlines the problem, the justification for the study and a description of the approach employed to produce the output and results of the study.

Chapter 2 '*Research Issues*', provides the literature review that supports the concepts that form the basis for this study. These concepts include the risk frameworks and governance frameworks that are commonly used to manage operational risk within the finance industry. It presents, explores and compares the different types of IT sourcing models used to delivery IT services. In Chapter 2 there is an investigation of the literature on decision theories commonly used to justify the selection of a specific IT sourcing model. A review of the governance models used to manage the different IT sourcing models is also discussed. Finally, from the information discussed in the previous sections of Chapter 2, the research questions for this study are presented. These theories, models and frameworks are brought together in the conclusion section of Chapter 2 to demonstrate significant gaps identified that lead to the development of the research questions and that are addressed in Chapter 4.

Chapter 3 '*Methodology*', provides the reader with details on how the analysis was carried out and why this approach was selected. This then leads the reader to

Chapter 4 '*Analysis of Data*', that guides the reader through the data sources used in the analysis and the results derived from the analysis. In Chapter 5 '*Discussion*', we provide the academic debate based on the extensive review of the relevant literature provided in Chapter 2 and the conclusions drawn from the results of the data analysis in Chapter 4.

The final Chapter 6 '*Conclusions and Implications*', provides the reader with a summary of the whole study and the implications of the study for theory and practice. Chapter 6 also directly addresses the research problem and propositions outlined in section 1.2. The limitations of this study are acknowledged and suggestions made for future research that can be addressed in a PhD research project.

1.8 Conclusion

This chapter has described the motivation for the study and provided the background to the environment of the study. The research problem and propositions have been outlined with the expected contribution and significance the study.

Finally the author has identified which information is needed, where the information is sourced, analysed and how the results are presented. In the next chapter the author will review in more detail the literature that underpins the concepts of the study and provides the academic foundation for this study.

Chapter 2 Research Issues

2.1 Introduction

Building on the previous chapter, this chapter examines the literature around risk management with a specific focus on prudential and operational risk management. The author has also reviewed the literature relevant to the different delivery models and the literature on decision theories commonly used to justify the selection of a specific IT service delivery model. An investigation was then conducted of the literature associated with the governance models used by organisations to manage the different types of IT service delivery models.

Figure 2.2 provides an overview of the structure of this chapter.

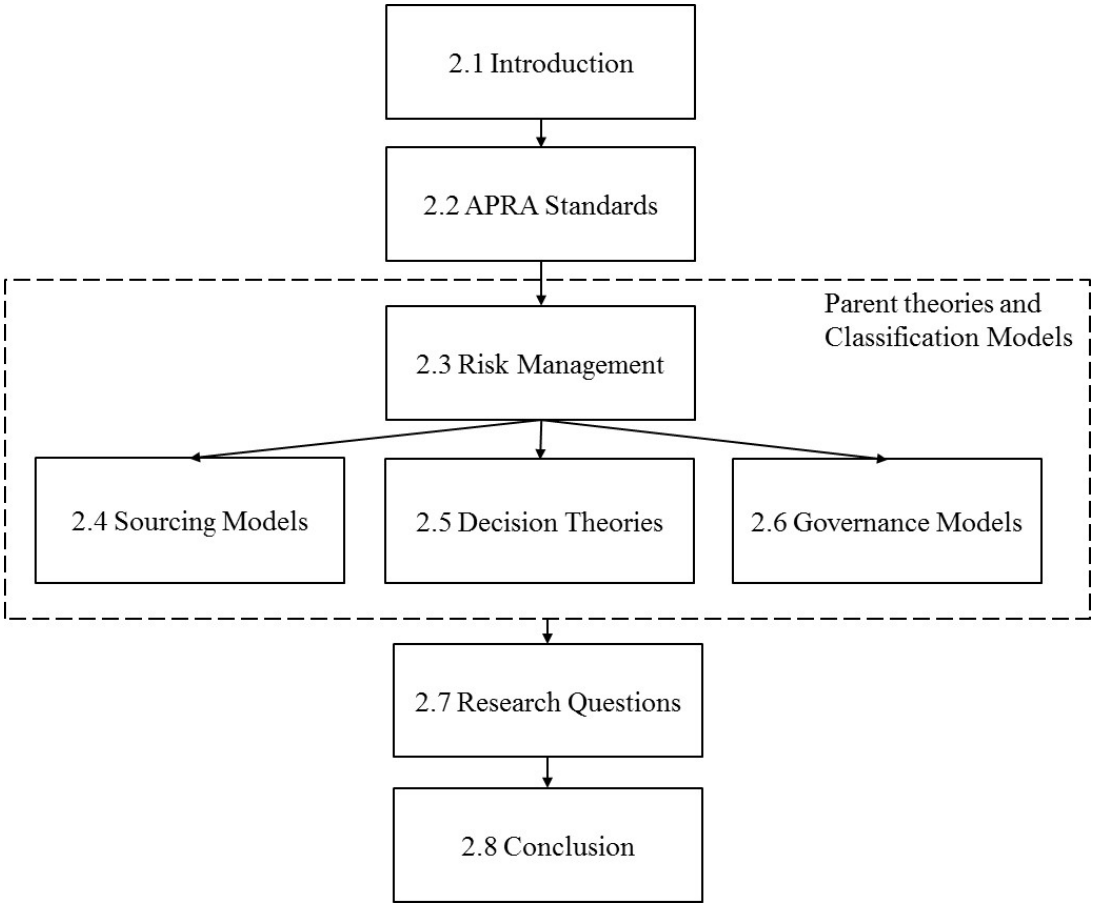


Figure 2.1 – Chapter 2 Structure

Section 2.1 provides the introduction to the chapter and lays the foundations for the chapter's structure and what is delivered by this chapter. Section 2.2 outlines and discusses the prudential standards used by APRA to govern outsourcing and operational risk management with the banks. Section 2.3 provides a discussion focused on risk management with the banking sector. Section 2.4 outlines and provides the definitions for the models used to deliver IT services. Section 2.5 investigates the decision theories that are referenced by academics and practitioners when formulating the justification for a particular delivery model that is defined in section 2.4. Next in Section 2.6 the author has reviewed the governance models that are recommended for each type of delivery model. Section 2.7 outlines the research questions that were developed during the literature review performed in section 2.2 to 2.6. Finally Section 2.8 provides a summary of the review and conclusions for this chapter. It also includes

any potential gaps discovered in the literature review and provides a link to the next chapter.

The first stage of the research was to conduct a systematic literature review to collect information from academic journals to build a comprehensive picture of the decision theories, risks and governance models that can be used to understand IT sourcing models used in the AFSI. To maintain consistency when searching for relevant journal articles, key words such as "prudential risk", "APRA", "Basel operational risk", "outsourcing risk", "outsourcing governance", "offshoring risk", "offshoring governance", "banks outsourcing", "banks offshoring" were entered in the 'Variable Parameter' section however the 'Static Parameters' such as "journal articles", "peer-reviewed publications", "English" section were not changed.

The study informed by the literature examined the theories underpinning the decision-making process that has a bearing on the banks' choice/s of IT sourcing delivery model/s. The researcher then identified the governance model/s and risk framework/s used to manage the different IT sourcing delivery models and associated risks. These three lenses (risk frameworks, governance models and decision-making theories) together provide a comprehensive picture of the banks' IT service delivery model in terms of IT sourcing.

Next the researcher used the banks' IT service delivery model as a foundation to review APRA's governance coverage of the banks' IT services sourcing strategies. Finally, the researcher evaluates the data on APRA's governance and the banks' IT services sourcing strategies to identify if any banking sector, AFSI or economic risk are not addressed under the current APRA prudential regulations for outsourcing and operational risk management (APRA 2005, 2006, 2013a).

A review of the APRA risk framework has established the foundation for building the industry level risk profile in the analysis of data (Chapter 4). The banking sector risk profile developed as part of Chapter 4 is used to ascertain whether or not current regulatory risk governance is sufficient to govern the economic risk associated with the banks' introduction of their IT multi-sourcing models. This banking sector risk profile informs the foundation of the study and builds a picture of the risks associated with the mix of service delivery models at the industry level.

2.2 APRA Standards

As stated in Chapter 1, regulatory governance of outsourcing is managed under the Council of Financial Regulators (CFR) framework. The CFR is consists of APRA (see APRA 2010), the Australian Securities and Investment Commission (ASIC), the Reserve Bank of Australia (RBA) and the Treasury Department of the Australian Government. APRA is legislated by the Banking Act 1959 (Australian Government 1959) to perform a prudential risk governance role within the AFSI and to enforce adherence to the Australian Prudential Standards (APS). The remainder of this section outlines and discusses the prudential standards that APRA use to manage outsourcing and operational risk within the banking sector of the AFSI. APRA employs two prudential standards to manage IT risk associated with outsourcing the IT component of the banking services delivered to their customers.

2.2.1 Prudential Standard APS 232

Firstly in April 2005 APRA released prudential standard APS 232. This standard details the requirements for business continuity management (BCM) services within the banks. The purpose of APS 232 is to provide guidelines on business continuity planning and management required to overcome IT disasters, with its main focus being

on the potential failure of IT infrastructure (APRA 2005). Although this prudential standard was not developed to address risks associated with IT outsourcing, APRA did link it to the outsourcing prudential standard it released the next year. The prudential standard released in 2006 was written specifically to address risks associated with outsourcing and is addressed in more detail in the next section.

2.2.2 Prudential Standard APS 231

The second prudential standard was released by APRA in October 2006. APS 231 provides the requirements for managing risk associated with the banks' outsourcing activities. APRA uses APS 231 to provide guidelines to banks' proposing to use outsourcing as a means of delivering IT services that the bank has the ability to provide (APRA 2006). One of the guidelines in APS 231 is to meet the requirements in APS 232 regarding business continuity plans (BCP) and the bank's BCP must be integrated with the external service provider's BCP before engaging into an outsourcing agreement.

The interpretation section of APS 231 states:

> "*For the purposes of this Prudential Standard, offshoring means the outsourcing by an ADI of a material business activity associated with its Australian business to a service provider (including a related body corporate) where the outsourced activity is to be conducted outside Australia. Offshoring includes arrangements where the service provider is incorporated in Australia, but the physical location of the outsourced activity is outside Australia. Offshoring does not include arrangements where the physical location of an outsourced activity is within Australia, but the service provider is not incorporated in Australia*" (APRA 2006, p. 2).

This statement highlights that APRA does not differentiate between offshoring and outsourcing in relation to risk management. The APS 231 statement forms the basis of the research from the regulator perspective.

2.2.3 Prudential Standard APS 115

A third prudential standard used in this study is APRA's prudential standard to govern operational risks: APS 115. APS 115 was released in 2103 and provides banks with guidelines for the assessment, management and reporting of operational risk (APRA 2013a). APS 115 aligns with the operational risk requirements in the Basel II capital accord produced by the Basel Committee on Banking Supervision (BCBS) (Basel Committee on Banking Supervision 2004). This prudential standard does not purely focus on outsourcing but all aspect of the banks' operations but it does reference the risks associated with outsourcing as being in scope of the risks addressed by this prudential standard.

This research evaluates the banks' IT multi-sourcing service delivery models and associated risks using these APRA prudential standards. This ascertains if the prudential standards (APRA 2005, 2006) and the APRA risk management framework documented in (APRA 2013a) provide sufficient proactive risk management coverage to govern the cumulative risks introduced by the banks' IT multi-sourcing strategies.

2.3 Risk Management

Comcover is a department within the Australian government that published a factsheet and guidelines paper that summarised the ISO 31000:2009 risk standard

(Australian Government Comcover 2010). Comcover provided the following definition of risk based on the ISO standard '*the effect of uncertainty on objectives*' and risk management as '*the management of the effect of the uncertainties*'. From an operational risk perspective, APRA implements the guidelines detailed in the Basel II capital accord published by the BCBS. The Basel Committee on Banking Supervision (2004, p. 149) 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*".

In a paper on governance and risk within UK banks, Alexander (2006) refers 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, p. 10). 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 for a company using an agent to deliver services is they may be attempting to move risk to the third party. Alexander's rationale is aligned with one of the concepts of agency theory that is to shift risk to the service provider. Alexander reviews the systemic risks associated with using an agent to deliver services. The impact can affect 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, p. 18). Alexander supported this statement by linking it to the Basel Committee statement on the importance of corporate governance within the banking industry to support national and global economic stability. Alexander recognises the role of a strong contract to manage risks associated with the use of services from an agent, but also pointed out the contract provides reactive risk protection but does not provide a mitigation of the risk.

In a paper on operational risk, Moosa (2011) investigated whether or not there was a link between operational risk and macroeconomic variables such as the unemployment rate. Moosa investigated whether operational risk is systemic and does it need the same governance as market and credit risk. Moosa argued operational failure in one institution may not have a '*domino effect*' resulting in an impact on the economy and therefore operational risk is idiosyncratic. Moosa attempted to link operational risk to cyclical events within the economy such as the rise and fall in the unemployment rates over a period of time. Moosa did not arrive at a definitive answer as to whether operational risk should be governed under the Basel accord in the same way as market and credit risk are governed. The analysis was performed on data over a period of time to identify relationships between operational variables and unemployment variables. Moosa's approach appears to assume a static operational environment. In contrast, our study provides projections on the potential economic impact resulting from operational changes in banks and the potential for critical failures of systems, processes or people when using offshoring as a major component of the banks IT multi-sourcing strategy.

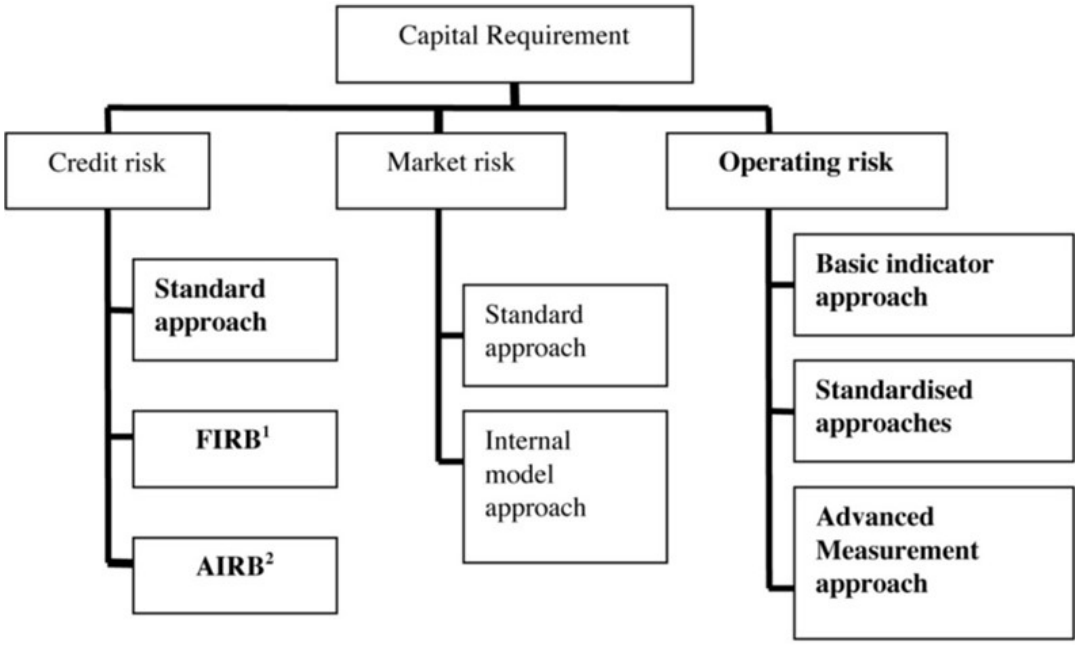
Another risk that is documented in the APRA prudential standards on outsourcing (APRA 2005, 2006) is the security of data. Mathew and Chen (2013) highlighted a risk associated with offshoring software development: the "*shirking and misappropriation of information assets*" (Mathew & Chen 2013, p. 299). This is a risk that, although addressed in the APRA outsourcing prudential regulations, is not addressed in APRA's risk prudential regulation (APRA 2013a).

Willcocks, Lacity and Kern (1999) conduced a longitudinal study into outsourcing within the UK defence sector. Their study has revealed the risks associated

with outsourcing and illustrated the need for the right governance model, the selection of the right service components to retain and outsource, building the contract that aligns with the governance model and the vendor selection process to select a the vendor that fits the companies' culture. Although focused on the risk associated with outsourcing the risks and the mitigation strategy, Willcocks et al.'s discussions are aligned with the risks associated with the banks and their multi-sourcing strategy.

2.3.1 Risk Management in the AFSI Banks

In the previous paragraphs the author has focused on the forms of risk (credit, market and operational) and the need for a risk framework to form part of the corporate governance framework required to manage the risks. The next step in reviewing risk management is to analyse the models that are used to measure and manage risk impact. In the banks Terry (2009) outlined the main methods of measuring risk and allocation of a capital value to that risk within the AFSI. Terry demonstrated the method of calculating capital requirements under Basel I and Basel II as shown in Figure 2.2



Notes: The new features (under Basel II) are shown in bold
[1] Foundation internal ratings based approach.
[2] Advanced internal ratings based approach.

Source: Terry, C. *The New Basel Capital Accord: A Major Advance at a Turbulent Time*, (2004 p.28).

Figure 2.2 – Capital Requirements under Basel I and Basel II.

As seen in Figure 2.2 risk can be grouped into three categories (credit, market and operational). In this study the author has focused purely on the operational 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 operational risk the Basel Committee has identified and recommended three methods of calculating risk capital allocation. The 'Basic Indicator Approach (BIA)' and the 'standard approach (SA)' are two risk capital allocation approaches that use a percentage of the gross income of the banks as the risk capital allocation. The third method is called 'Advanced Method Approach' (AMA) and requires the bank to have a robust risk

framework approved by APRA and a system that can quantitatively estimate and model risk based on internal and external historical operational risk data (Terry 2009). Both CBA and WBC are approved to use AMA for the calculation of their capital allocation for operational risk.

The Chairman of APRA, Dr John Laker (2008) outlined how APRA has adopted and was implementing the Basel II framework. He stressed that APRA would not facilitate ADI's '*cherry picking*' of the capital allocation methods they would be able to use. APRA recommends that ADIs seeking APRA accreditation adopt AMA for operational risk assessment and must also adopt the internal ratings-based (IRB) assessment method to calculate risk allocation. APRA issued two prudential standards in January 2013 that address the risk framework and capital adequacy for both the standardised and advanced measurement approaches. APS 114 (APRA 2013b) outlined how capital allocation is measured using a standardised measurement for operational risk. APS 114 (APRA 2013a) articulates the advanced measurement of calculating capital adequacy and also the risk framework that ADIs must adhere to in order to meet the Basel and APRA requirements.

Effective from the 1st January 2008 both CBA and WBC were approved to use the Advanced Measurement Approach (AMA) under Basel II and the capital framework to manage operational risk (Basel Committee on Banking Supervision 2004). The APRA Prudential Standard implemented in 2013 required the banks to use and be audited based on specific conditions (APRA 2013a) which is a direct localisation in Australia of the Basel II requirements for operational risk management as documented in the Basel II Accord released in 2004.

The following sections 2.3, 2.4 and 2.5 review the literature on sourcing models, decisions theories and governance models. Each of the models and theories introduce different operational risks. These operational risks provide the basis for an in-depth analysis of the secondary data in relation to these different operational risks in Chapter 4.

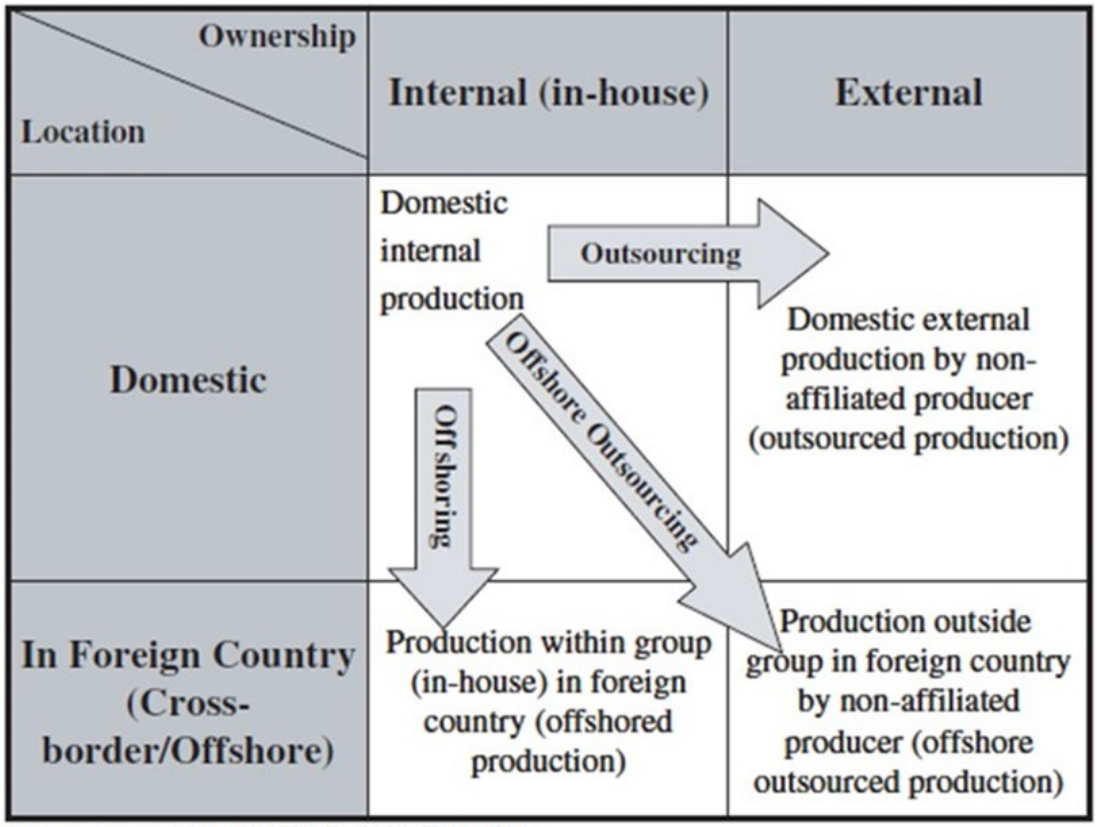
In Chapter 5 there is an in-depth discussion of the use of AMA and whether or not there could be other risk evaluation methods that might be more applicable to operational risk and more specifically IT operational risk in relation to IT sourcing and specifically multi-sourcing methods to deliver IT services.

2.4 Sourcing Models

Dibbern et al. (2004) provided a decision-making framework on IS outsourcing that explained the "'*why to outsource', 'what to outsource', 'which decision process to take', 'how to implement the sourcing decision' and what is the 'outcome of the sourcing decision'*" (2004, p. 6). Dibbern et al. presented the reasons a company use when justifying what more they can achieve by outsourcing IS rather than providing the services in-house. The paper provides an extensive history of the evolution of outsourcing and contributes to our understanding of the decision and selection process behind the selection of this as an IS delivery model. The paper is extensive and would form a relevant basis if we were discussing the decision theories behind outsourcing and other forms of sourcing. In this study we are focused on the theories that inform the statements published by the banks to justify their decision, not the decision-theories that formed the original strategy. For this study we focus the discussion on the banks' use of multi-sourcing (a combination of outsourcing, offshore-outsourcing and in-house) as their method of delivering IT services and the associated risk with their decision.

As highlighted by Raman and Chadee (2007) considerable research has been conducted on this relatively new phenomenon of international outsourcing or offshoring of information technology services by advanced industrialised countries to less developed countries. However, *"given the multidisciplinary nature of the subject, the literature on offshoring is often disparate and subject to confusion*" (Raman & Chadee 2007, p. 1). In a later paper on international outsourcing by Chadee and Raman (2009) this position was restated and their literature research reinforced and affirmed the statement in their paper published in 2007.

Various lenses have been used to view sourcing delivery models e.g. Lacity, Khan and Willcocks (2009) provided an extensive review of outsourcing and the associated literature. They also touched on offshore-outsourcing as a new phenomenon. Tate et al. (2009) reviewed the trend of offshore-outsourcing using nine case studies to demonstrate the evolution of offshore-outsourcing. Lane and Van der Vyver (2006) reviewed the pros and cons of using offshoring as a means of delivering IT services. For the purpose of this research project, the author has adopted the outsourcing and offshoring matrix illustrated in Kirkegaard (2008) that was originally developed by UNCTAD. Figure 2.3 shows how the different delivery models relate to each other and to the company.



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

Figure 2.3 – The Standard Offshoring and Outsourcing Matrix

Figure 2.3 presents four distinct models to deliver services: in-house; outsourcing; offshore-outsourcing and offshoring. Outsourcing refers to the provision of services domestically by an external service provider. Offshore-outsourcing relates to services provided from an international location by an external service provider. In-house is where services are provided from within the company and in a domestic

location. Offshoring relates to services provided within the company from an international location by an internal service provider.

In this study the author has focused on the risks associated with outsourcing, offshore-outsourcing and in-house. In Chapter 4, the analysis, a risk profile is provided for each bank and the industry level that demonstrates that each IT services delivery model carries a different risk profile. As part of the analysis, this risk profile model is developed to show the industry level IT services model effect. This adopted model is used in the development of the risk profile model that demonstrates any AFSI risk exposure associated with the banks' sourcing decisions.

2.5 Trends

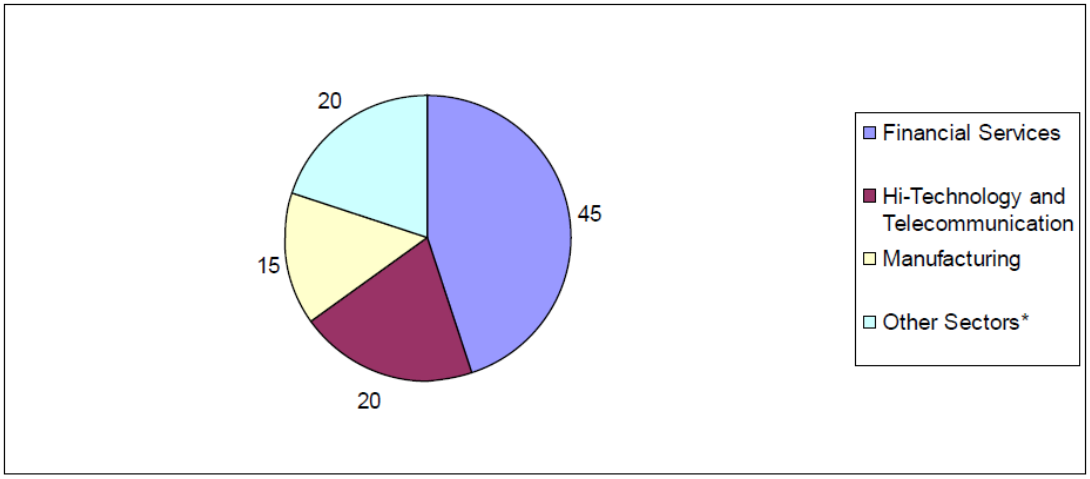
Palugod and Palugod (2011) examined the drivers influencing the decision to outsource and offshore and the operating models that are adopted as a result. Palugod and Palugod drew on data produced by Cap Gemini (2007) on outsourcing trends between 2007 and 2012 within the retail banking sector, as displayed in Table 2.1. The following definitions of the three elements in Table 2.1 were provided by Palugod and Palugod (2011, p. 15): "*IT functions include operations, maintenance and development*"; "*Back Office functions including payments, life insurance, mortgage, consumer credit*"; and "*Support Functions including accounts payables, accounts receivables, human resources, treasury, procurement, property management, and general ledger*".

Table 2.1 – World Retail Banking Report, 2007

% of Banks that Outsource	2007	2012
Back Office	58%	65%
IT	58%	65%
Support Functions	27%	40%

Source: Cap Gemini, World Retail Banking Report, 2007

For this study, the figure of greatest interest in Table 2.1 is the increasing outsourcing trend forecast for IT. It was estimated this trend would increase by seven percent in a five year period. As part of this study we present a comparative trend analysis for each of the banks that shows if the trend shown in Table 2.1 aligns with our study period 2009 to 2014. The other data source Palugod and Palugod draw on in their investigation was produced by Everest (2008) and was on the segmentation of offshoring by industry and utilisation of offshoring as a delivery solution as illustrated in Figure 2.4.



Source: Everest Institute, 2008

Figure 2.4 – Offshore Adoption Rates by Industry, 2007

Figure 2.4 shows across industry sectors a sample of companies in 2008 that used offshoring as a means of delivering services. It can be seen from Figure 2.4 that the financial services industry had the highest percentage of utilisation of offshore delivery (i.e. 45 percent) out of the sample. From the data this study verifies if the trends presented by Palugod and Palugod in 2011 are similar to outsourcing trends occurring within the AFSI. This study proposes to analyse and present how the increased utilisation of IT offshoring as a delivery model has changed the risk profile within AFSI.

Although purely focused on IT outsourcing, Beaumont and Costa (2002, p. 16) highlight one of the disadvantages of outsourcing IT is the potential for the "*loss of distinctive competencies*" as a consequence of the knowledge transfer process. It is difficult for a company to protect its intellectual property (IP) from an outsourcing company as the IP is built into the software design and ongoing development (Beaumont & Costa 2002). Beaumont and Costa also point out that the transfer of IP could create the opportunity for the outsourcing company to produce its own product and sell this to new entrants into the market. If Beaumont and Costa are correct about the potential loss of distinctive competencies through IT outsourcing, the banks' risk of losing their competitive advantage could be higher in using an IT offshore-outsourcing model. How do the banks ensure their IP is protected and secure from misuse by the service providers when they are delivering banking solutions to other customers outside the AFSI? Do the banks' Business Continuity Plans cater for the loss of IP from events outside their control, such as service provider takeovers or collapse? It is worth noting that most IT offshore-outsourcing service providers have their own banking products that they sell to other banks.

2.6 Decision Theories

Raman and Chadee's (2007, p. 3) review of the literature on offshoring of IT services argued "*research on various aspects of offshoring to date have tended to draw from three broad streams of theoretical literature; namely (1) strategic management, (2) economics and (3) economic sociology*". These streams are discussed in the following sections.

2.6.1 Strategic Management Theories

Resource Based View Theory (RBV) (Barney, Wright & Ketchen 2001), argues that company resources form part of the company's competitive advantage and having

resources with the right set of skills is an important part of the company's competitive advantage. This infers that a major component of the company's sourcing strategy is to ensure the availability of these skilled resources and is a key decision driver. This position is also supported by other researchers in sourcing decision-making e.g. Tate et al. (2009). Knowledge-Based Theory (KBT) (Alavi & Leidner 2001) purports that knowledge-based resources influence the company's ability to maintain its competitive advantage. One of the main activities an organisation has to perform during the transition phase to an offshore-outsourcing model is the knowledge transfer (KT) process. The KT process involves moving knowledge from the company's resources to the service provider resources and storing the information in a digital format. This poses some risk around the management of the digital knowledge and security for the AFSI. These risks are addressed through the risk analysis phase of the study. KBT builds on RBV (Barney, Wright & Ketchen 2001) and is supported as a prime decision-making theory for understanding outsourcing and offshoring (Hätönen & Eriksson 2009; Herath & Kishore 2009; Whitaker, Mithas & Krishnan 2010).

2.6.2 Economic Theories

Transaction Cost Economics (TCE) (Coase 1998) argues the main decision-making driver is the company's cost of producing products or services. It is argued that outsourcing the production of products or services can reduce the transactional cost of producing the product or service. However it does require a strong enforceable contract to ensure savings are achieved. In this context, the contract is represented by the banks' Master Service Agreement (MSA). Other researchers have applied this theory to understand the key decision-making processes involved in outsourcing and offshore-outsourcing of IT services (Bunyaratavej et al. 2011; Hätönen & Eriksson 2009; Herath & Kishore 2009; Jahns, Hartmann & Bals 2006; Kedia & Mukherjee 2009; Ørberg Jensen & Pedersen 2011; Roza, Van den Bosch & Volberda 2011; Srivastava & Teo 2012; Stratman 2008; Tate et al. 2009; Whitaker, Mithas & Krishnan 2010; Willcocks 2011). The drive to offshore-outsource IT services is one of the main cost saving strategies adopted by the banks (Bennet 2012).

Agency Theory (Eisenhardt 1989), refers to the situations when a company uses a third party to deliver products or services on their behalf. Eisenhardt argues one of the rationales underpinning the use of a third party to deliver services is to shift risks associated with delivery to the third party. The key question addressed by this research is *does adopting a third party to deliver service mitigate the risk or simply shift the ownership of the risk?* This question is discussed further in relation to the APRA prudential regulation on outsourcing (APRA 2006) in chapter 6 section 6.5.In line with TCE, agency theory relies on a strong enforceable contractual agreement and governance arrangements to ensure quality and costs savings are achieved (Bunyaratavej et al. 2011; Hätönen & Eriksson 2009; Herath & Kishore 2009; Whitaker, Mithas & Krishnan 2010). If an upward trend in IT offshore-outsourcing within the AFSI is shown from the analysis. One could link agency theory as one of the main theories that could help explain the decision by the banks' to move from an IT outsourcing delivery model to an IT offshoring-outsourcing delivery model.

As part of the data analysis presented in chapter 4, the researcher demonstrates any correlation between the banks IT services expenditure patterns with external IT services provider/s to the expenditure patterns on internally delivered IT services. The data from the analysis of each bank is plotted to evaluate if there is an expenditure trend that may have an influence on the banks' risk exposure due to a dramatic increase in the percentage of expenditure on externally purchased IT services.

2.6.3 Economic Sociology Theories

Decisions can be influenced by 'fashion setter' organisations such as consulting firms or competitors. This is referred to as 'Management Fashion Theory' (Abrahamson 1991, 2011). Abrahamson's Management Fashion Theory aligns with industry knowledge that shows the banks rely heavily on a small number of consulting firms when developing their sourcing strategy. The AFSI industry is quite small and senior personnel tend to move between the four major banks. This practice may have an influence on the decision-making processes as the executives transfer the knowledge, experience and skills gained in their previous institution to the new institution resulting in imitation within and between banking processes.

2.7 Governance Models

Jahns, Hartmann and Bals (2006) conducted a detailed review of the decision-making theories underpinning the selection of an offshore-outsourcing model. Jahns, Hartmann and Bals found the main theories explaining the decision to utilise offshoring as a delivery model were Transaction Cost Economics (TCE) (Coase 1998) and Resource Based View Theory (RBV) (Barney, Wright & Ketchen 2001). Jahns, Hartmann and Bals also analysed the governance models used to manage offshoring delivery and found that the governance model needs to be fluid to reflect each stage of the contract maturity cycle. This is an important factor in developing the AFSI risk profile. A mix of governance models within the individual banks could also influence the AFSI risk profile.

Smith (2002), a journalist with MIS Australian, examined how organisations could manage their outsourcing contracts to address service providers' shortcomings and make sure the customer receives the level and quality of services. Smith argued that a customer should ensure the contract covers all the requirements of the organisation and that a governance methodology is established to monitor services and take corrective action if required. From personal knowledge obtained as part of the commercial team of both banks and a preliminary review of the annual reports, it is clear that both banks have built their governance models into their MSAs. This may result in challenges when modifications are required to the governance model, as legal changes to the contract may also be required. Changes to an MSA could incur high legal and commercial costs and involve a considerable amount of time to take effect as such MSA contracts are complex legal documents that generally span more than one legal jurisdiction.

The investigation carried out by Smith (2002) uncovered two main strategies adopted by Australian IT Directors when establishing a service provider governance model, namely, the contestable strategy and the partnership strategy. Firstly, contestable strategy refers to leveraging the fact that there are many service providers in the market place competing for business. The customer organisations use this competition as a means of control. This works well with commodity items e.g. technology refresh (renewing technology) or implementation projects. The second approach, the partnership strategy, is effective when the services are associated with a longer term service contract such as Enterprise Resource Planning (ERP), software application development and support. This strategy may change to a contestable strategy when the contract needs to be renewed. If the partnership has been successful, the incumbent has a distinct advantage over other competitors in the market. Current industry knowledge reveals the banks use a combination of contestable and partnering as part of their vendor management strategy. Further evidence to support this claim is sought during the data analysis stage of the study.

A study of regulatory governance in the UK finance industry focused on the role of the financial regulator in managing economic risk by the enforcement of strong corporate governance (Alexander 2006). Alexander used the principal-agent model to explain the relationship between the banks and providers. Alexander concluded that the financial regulator needs to provide the banks' with a flexible risk governance framework in order for them to manage the economic exposure caused by the UK banks' decisions to utilise agents to deliver services.

In the Laurent (2006) article on outsourcing governance, two important corporate governance and offshoring success factors were identified. Firstly, regulatory governance is not static and therefore the corporation needs to evolve its governance strategy as technologies and regulations change. Secondly, it is important to have a contractual framework that can be modified as corporate and industry regulations change (Laurent 2006). A historical study of outsourcing by Willcocks (2011, p. 5) purported that over the following few years one of the major success factors of outsourcing as a delivery model for IT services would be a move to a governance model based on trust and collaboration rather than an adversarial governance model based on sanctions. This again highlights the need for strong governance based on collaborations between the corporation and the service provider. Willcocks fails to address how a collaborative governance model coexists with the competitive tension experienced in a contestable governance model. It is this tension that the AFSI needs to address.

The focus of the Lane and Van der Vyver (2006, p. 1135) study was on offshoring in the Australian financial services industry. They argued "*Large scale off-shoring of IT could result in a shortage of skilled domestic IT professionals in developed countries like the USA, Europe and Australia if IT is perceived as a career with no future*". This argument supports the assertion that a lack of APRA governance of the banks' offshore-outsourcing activities could have a negative economic effect in both short and long term. Another risk factor identified is the case whereby a bank is forced to react to an overseas situation and needs to repatriate the IT services managed under an offshore-outsourcing. Lane and Van der Vyver (2006) discuss an example of a bank using an offshore delivery model where the offshore delivery centre is owned and controlled by the bank (captive). In this scenario the bank has more control over how the repatriation of IT services is performed due to economic changes. A bank using the offshore-outsourcing model to deliver its IT services lacks this control except through the enforcement of legal clauses in their MSA. As the service providers are headquartered in other countries, legal action could take extensive time with the multiple legal jurisdictions involved. During this time the bank's reputation and consequentially consumer confidence could be negatively impacted and this could have a domino effect across the AFSI.

Another important link between governance, decision theories and the success of offshore-outsourcing is that the contracts need to take into account more than legal and commercial requirements and should also align with the original decision-making drivers (Benit et al. 2010). Benit et al.'s position is also supported in the review by Bunyaratavej et al. (2011) on the multi-discipline aspects of offshoring governance.

Another aspect of governance highlighted by Ørberg Jensen and Pedersen (2011) suggests governance also needs to align the type of services being purchased and the strategic value the corporation put on these services. The governance of core services requires tighter control than non-core (commodity) services. The corporation's strategic drivers should also align with the service providers' in order to create a workable model (Whitaker, Mithas & Krishnan 2010).

Simon, Poston and Kettinger (2009) investigated the successful implementation of offshore-outsourcing and developed a maturity governance framework. Srivastava and Teo (2012) found a strong alignment between the type of delivery model used and the type of governance, for example outcome based models require formal controls through contracts, however, time and material contracts could be managed by informal controls, such as shared goals and self-governance.

Finally another part of governance that can influence the success of an outsourcing contract to purchase services from an external service provider is the use of frameworks. These frameworks range from company specific such as balanced scorecards to global frameworks and standards such as Capability Maturity Model Integration (CMMI), Six Sigma, IT Infrastructure Library (ITIL) and Control Objectives for IT (COBIT). These frameworks allow the customer to establish common benchmarks across external service providers who provide services within the same discipline e.g. infrastructure, application development, service desk services etc. Wilkinson (2006) investigated the uses and challenges of using industry standard frameworks in an IT governance model and found it does increase stability and provide a framework of common understanding. The challenge comes where the customer is at one level of maturity and the external service provider is at another level within a framework. This maturity level misalignment could lead to misunderstanding or misinterpreting customer requirements.

2.8 Research Questions

Based on the academic and practice theories and models examined in this chapter the following research questions are formulated in this Masters dissertation:

RQ1. Do the banks employ complex multi-sourcing solutions driven by business unit demands to deliver their IT services?

RQ2. What are the risk and governance model/s used by the banks to manage risks associated with their IT services multi-sourcing strategy?

RQ3. Is the AFSI IT operational risk exposure adequately covered by the current APRA risk framework and prudential standards?

2.9 Conclusion

The literature on ‘outsourcing’, ‘offshore-outsourcing’ and ‘offshoring’ is diverse (Raman & Chadee 2007). The theories that attempt to explain decision-making on sourcing models is extensive and complex (Raman & Chadee 2007; Roza, Van den Bosch & Volberda 2011). Governance models adopted to manage the quality and risk associated with an offshore service provider is shaped by a range of decision-making theories (Stratman 2008). Cultural alignment between the contracting organisation and the service provider organisation is an important factor in the decision-making and governance process (Jahns, Hartmann & Bals 2006; Roza, Van den Bosch & Volberda 2011). All of these factors are used as inputs to build the risk profile for the AFSI that can be utilised to reveal and analyse any potential gaps not covered by APRA’s regulatory framework.

Table 2.2 summaries the review of the literature on decision theories used to justify one or more sourcing models.

Table 2.2 – Cross Reference of Decision Theories and Sourcing Models

Decision Theories	Sourcing Models	
	Outsourcing Number of Research papers	**Offshore-Outsourcing** Number of Research papers
Transaction Cost Economics	11	17
Agency Theory	11	11
Knowledge-Based Theory	4	5
Resource Based View Theory	4	4
Management Fashion Theory	1	0

From the data presented in Table 2.2 it can be seen that the dominant theories used when researching outsourcing and offshore-outsourcing are transaction cost economic (TCE) (Coase 1998) and agency theory (Eisenhardt 1989). TCE theory was found to be more dominant in the literature reviewed to understand offshore-outsourcing. Both TCE and agency theory were equally relevant when used in studies focused on the selection of outsourcing.

These theories help to explain the type of governance model employed to manage service provider engagement in outsourcing and offshore-outsourcing arrangements (Alexander 2006; Jahns, Hartmann & Bals 2006).

Consequentially, this research draws on these theories and the IT governance models as the foundations for the risk analysis performed on the data gathered from the banks. The other theories discussed in the literature may help explain the banks' decision making process; evidence to support this is identified during the data analysis stage of this study.

The literature review revealed a number of gaps. Firstly, there is scant literature applying decision theories and governance models to research banks' use of multi-sourcing strategies for the delivery of IT Services. A further gap reveals a lack of research focusing on AFSI regulatory and risk governance of the banks' IT multi-sourcing strategies.

No evidence was found other than statements published in the bank's own media releases stating the reasons for using outsourcing, outsourcing-offshoring or a combination of service models to deliver IT services. To provide definitive reasons that would allow us to test a specific decision theory we would need to interview the decision makers in each bank. In this chapter we explored the dominant theories that have been shown in other countries and businesses to inform making the decision to use outsourcing, outsource-offshoring or a combination of delivery models to achieve the goals of the business. In chapters five and six we do link decision theories to the results of chapter four through association that provides a foundation for future study into this area.

The important output from this chapter is the investigation into the prudential instruments used by APRA, risk management currently used and the governance model discussion. In the governance review we investigated the frameworks and models, these link directly to the output from chapters four, five and six and provide a clear link back to the discussion in this chapter.

Chapter 3 Methodology

The methodology chapter provides the details on how the project scope and approach were developed and why. Figure 3.1 provides an overview of this chapter.

3.1 Introduction

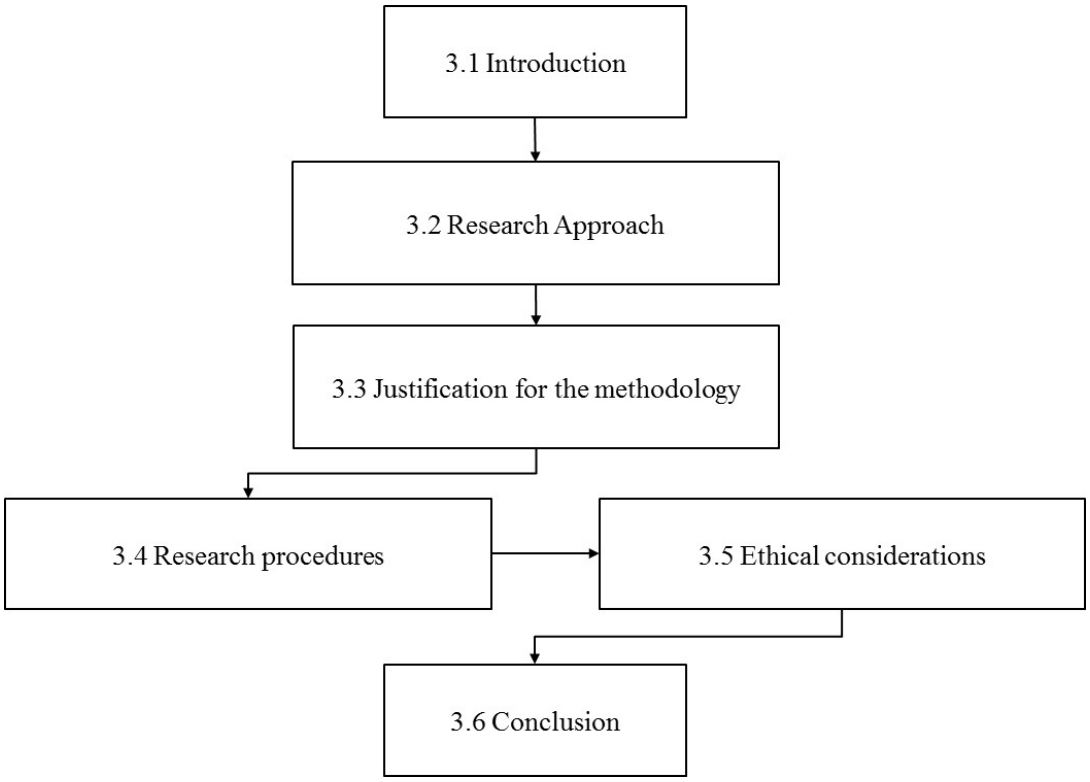


Figure 3.1 – Chapter 3 Structure

Section 3.1 provides the introduction to the chapter and lays the foundations that was delivered and the structure of the chapter. Section 3.2 outlines in detail the research approach and details the data collection approach that was taken to ensure total coverage of the data collected from the sample. Also this section walks the reader through the data analysis approach used to develop the results to answer the research questions. Section 3.3 provides the justification for the methods used in the study. Section 3.4 provides details on the procedures used to collect and analyse data in the study. Section 3.5 explains the ethical considerations that form part of the study. Section 3.6 provides a summary of the chapter along with a link to the next chapter of the dissertation.

3.2 Research Approach

This study is based on a five year longitudinal case study of two banks: WBC and CBA. The research sourced information from academic publications, information in the public domain made available by the banks, external service providers, consultancy companies, APRA, BCBS and other Australian government agencies. Figure 3.2 shows the data sources that were used and the type of information that was collected to perform qualitative analysis in a systematic manner using a qualitative data analysis tool (NVivo) in order to provide answers to the research questions.

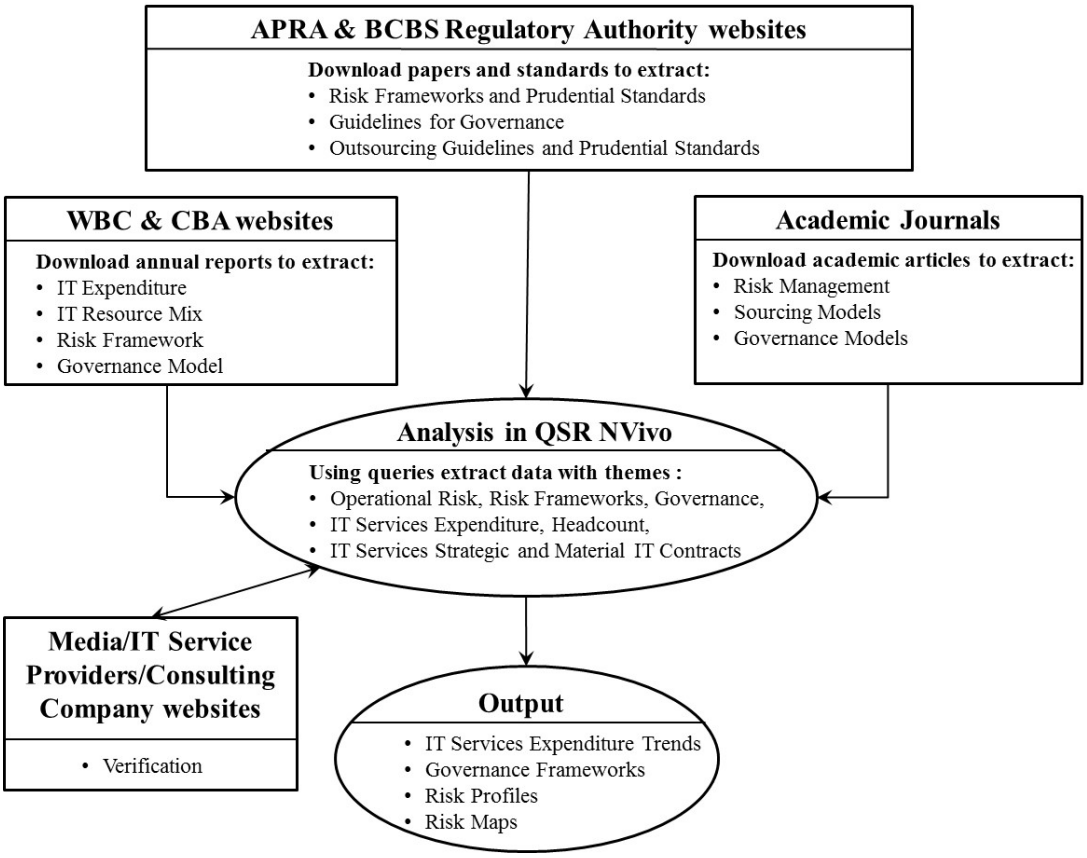


Figure 3.2 – Data Collection and Qualitative Data Analysis Approach

The research extracted information from academic publications, and information in the public domain made available by the banks, APRA, BCBS and other government agencies websites. The information extracted from the banks' websites was verified via media, service providers and consultancy companies' websites. Searches of the banks' web sites were conducted to identify available data relating to the banks' IT services delivery landscape and risk frameworks and governance models employed to manage the delivery of IT services.

Academic databases were searched to identify journal articles relating to financial industry regulators' and governance models used to manage IT services risk. The author has also reviewed journal articles on IT services sourcing models and decision theories used within the banking industry as part of the selection process of an IT services sourcing model.

A search of IT service providers, media publications and consultancy company websites was used to supplement and verify the information gathered from the banks' and government web sites specific to the AFSI. The sources for the research data are shown in Table 3.1.

Table 3.1 – Data Sources

Organisation	Source - website	Information
Banks		
CBA WBC	www.commbank.com.au www.westpac.com.au	Annual reports, media releases, risk framework, governance frameworks
Government / Regulatory		
APRA BCBS	www.apra.gov.au www.bis.org	Risk framework, Governance frameworks, regulations and communications on outsourcing and offshoring
Academic		
USQ	http://usq.summon.serialssolutions.com	Journals on decision theories, governance models, risk theories and models associated with 'outsourcing', 'offshoring' & 'offshore-outsourcing'
Newspaper & publications		
AFR The Australian CIO	www.afr.com www.theaustralian.com.au www.cio.com.au	Articles on Australian banks outsourcing or offshore IT functions
Service Provider		
TCS Infosys Wipro HCL IBM GSA	www.tcs.com www.infosys.com www.wipro.com www.ibm.com www.hcltech.com	Verification of information gathered from the banks
Consulting Companies		
Deloitte KPMG PwC AT Kearney	www.deloitte.com www.kpmg.com www.pwc.com.au www.atkearney.com	Verification of information gathered from the banks

The content of all reference materials:

1. 10 bank annual report with 2,720 pages;
2. 14 regulatory documents with 559 pages; and
3. 14 media documents with 143 pages;

was extracted from the public domain and stored as a QSR NVivo project. A folder or set structure was created to segregate the subjects of the literature. QSR NVivo was used to perform a systematic and rigorous content analysis (Krippendorff 2013) which in turn was used to develop answers to the three research questions.

To undertake the analysis of the banks' IT multi-sourcing strategic activities, the author extracted the annual reports from 2009 to 2013 and gathered information on the annual IT spend, employee headcount, IT headcount, IT contracts that were either signed or formed part of the bank's strategic plan. Analysis was undertaken to review and deconstruct the risk management framework adopted by each bank to enable a comparative study that demonstrated the alignment and misalignment of the risk frameworks between the banks and the guidelines provided by APRA. Further analysis

involved reviewing the data available from the banks' websites, media centres for press releases from 2009 to 2013 relating to IT projects or IT service contracts signed with IT service providers. This information created a picture of each banks' profile including trend information about IT employee numbers, IT spend and IT service provider engagements. The author considered interviewing each bank's CIO, but due to the sensitive and confidential nature of IT service provision the decision was made to commence the analysis with documents in the public domain rather than relying on opinions which may be subjective and unreliable.

The research was performed in three stages.

In stage 1 a review of the media releases, banks' annual reports and service provider sites was carried out. A template to describe the sourcing landscape of the banks has been created as shown in Table 3.2.

Table 3.2 – Sourcing Landscape of the Banks

	CBA Method of Delivery				WBC Method of Delivery			
	Outsource	Outsource Offshore	Offshore	In-house	Outsource	Outsource Offshore	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								

In Stage 2 the author populated the sourcing trend analysis template shown in Table 3.3 with the trend data extracted from the banks' annual reports. Tables 3.2 and 3.3 were developed to provide a comprehensive summary of the banks' IT demographics and IT Service provision from 2009 to 2013 to inform the next stage of the project.

Table 3.3 – Sourcing Trend

Human Resource Data	2009	2010	CBA 2011	2012	2013
Total FTE Headcount					
IT FTE Headcount					
IT Contractors					
Total FTE					
Human Resource Data	**2009**	**2010**	**WBC 2011**	**2012**	**2013**
Total FTE Headcount					
IT FTE Headcount					
IT Contractors					
Total FTE					
IT Spend in millions AUD$	**2009**	**2010**	**CBA 2011**	**2012**	**2013**
Internal					
Outsourced Services					
Outsourced-Offshoring Services					
Total					
IT Spend in millions AUD$	**2009**	**2010**	**WBC 2011**	**2012**	**2013**
Internal					
Outsourced Services					
Outsourced-Offshoring Services					
Total					

In stage 3 the sourcing trend and landscape data collected for the CBA and WBC were used to populate the risk profile (Table 3.4) with information such as the IT service provider mix, critical IT projects and mix of IT service delivery model/s.

Table 3.4 – Risk Profile

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

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 2013a, pp. 26-30). 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 relationship between the APRA category 2 risk management component and the risk management component in Table 3.4 is a one to many relationship. Appendix 1 – Cross Reference to Risk Component contains a table that shows the relationships between the APRA categories to risk component names used in this study.

The '*Risk Owner*' listed in Table 3.4 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 annual reports (CBA 2009, 2010, 2011b, 2012, 2013) the owner within the bank of a risk component was identified according to which section of the annual report the risk component was addressed. If the ownership of specific risks was not consistent across the banks this could potentially add further risk to the component list at the AFSI level.

The '*Impact Rating*' or each '*Component of Risk Management*' listed in Table 3.4 is derived by different calculation methods (see Table 3.5). 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 on political, religious or economic unrest in the countries that services are delivered from to the bank. 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.

Table 3.5 – Measurement of Impact Rating

Component of Risk Management	How Impact Rating is Derived	Impact Rating	Measure
Governance and Risk Management	Established by APRA's prudential standard APS 115 attachment E	Low Medium High Very High	Governance and risk management need to be tested to demonstrate they provide the protection they were designed for. Similar to annual BCP testing that proves through scenario and simulations testing that the business can withstand a catastrophic event. Very High = No Testing completed. High = 1 Test in five years completed. Medium = 1 Test completed in 3 years. Low = Test completed annually.
Skills and Knowledge Management	Forms part of the banks' modernisation programs moving toward a services management model	Low Medium High Very High	1 to 5 Projects 6 to 10 Projects 11 to 15 Projects 16 or more Projects
Companies fit and Alignment	Tight selections process involving delivery and commercial, level established by reviewing the selection process outlined in the bank reports	Low Medium High Very High	A published vendor selection process that shows how validation of service provider's maturity and stability was performed based on measurements such as attrition rate. Very High = No published process. High = Published but in use for less than 3 years. Medium = Published and used for more than 3 years. Low = Published use with all vendors and results are published annually.

(Table 3.5 – Continued)

Component of Risk Management	How Impact Rating is Derived	Impact Rating	Measure
Quality Management	Process adherence to an established framework such as CMMi, ITIL as part of a services management model.	Low Medium High Very High	10 or more years 7 to 9 years 4 to 6 years Less than 3 years
Sovereign Risk / On-Going concern	Risk exposure reviewed on the basis of stability in the countries used to deliver services. Economic measures, political risk, religious mix.	Low Medium High Very High	Impact always high for countries with a mix of extreme politics based on religious extremism and where the wealthy to poor gap is high
Offshore facilities (capacity for growth)	Risk exposure reviewed on the basis of stability in the countries used to deliver service.	Low Medium High Very High	0 offshore delivery centres 1 offshore delivery centres 2 offshore delivery centres 3 or more offshore centres
Commercial	Number and complexity of contracts and SLAs.	Low Medium High Very High	1 IT services contract 2 IT services contracts 3 IT services contracts 4 or more IT services contracts. This component targets the number of commercial framework/s (agreement / contract) employed by the bank's commercial business unit to manage IT services and/or external service providers.
Sustainability	Number of offshore service providers versus in-house.	Low Medium High Very High	100% in-house Less 50% offshore More 50% offshore 100% offshore

(Table 3.5 – Continued)

Component of Risk Management	How Impact Rating is Derived	Impact Rating	Measure
Critical projects	Number of modernisation programs utilising either offshore locations for services or offshore resources brought onshore to complete the work.	Low Medium High Very High	1 to 5 IT projects 6 to 10 IT projects 11 to 15 IT projects 16 or more IT projects
Data Leakage and Confidentiality	Data accessed only from within the locally controlled environment versus a mix of access from within the locally controlled environment and offshore delivery centre accessing data from the locally controlled environment.	Low Medium High Very High	100% onshore Less 50% offshore More 50% offshore 100% offshore
Service Provider Mix	Number of External Service Providers providing critical project resources and / or services.	Low Medium High Very High	1 IT service providers 2 IT service providers 3 IT service providers 4 or more IT service providers

The '*Probability Rating*' for each '*Component of Risk Management*' listed in Table 3.4 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, Yeung and Hong (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 scale of the impact ratings and probability ratings range is low, medium, high and very high with an associated value (1-4) to allow them to be plotted on the risk map shown in Table 3.6.

Table 3.6 – Risk Map

Bank /AFSI					
Impact Rating	Very High	VHL	VHM	VHH	VHVH
	High	HL	HM	HH	HVH
	Medium	ML	MM	MH	MVH
	Low	LL	LM	LH	LVH
		Low	Medium	High	Very High
		Probability Rating			

The combined risk mapping range shown on the risk map (Table 3.6) is from **LL** = (Low impact rating + Low probability rating) in the bottom left to **VHVH** = (Very High impact rating + Very High probability rating) in the top right. There is a risk profiles (Table 3.4) with an associated risk map developed from the risk profile as shown in Table 3.6 for each bank. The risk map enables a comparative analysis of risk management framework used in each bank. Finally a consolidated risk profile and risk map is developed to show the industry level risk position.

These AFSI specific risk artefacts could be used in a future study when interviewing representatives of the banks and APRA. Using a risk map developed from data available in the public domain enables a more objective discussion based on empirical data rather than subjective interviews based on open ended questions.

Both the risk profile and risk map were used to demonstrate the current risks within each of the banks and the projected AFSI risk map. The risk model can be used in a future study to demonstrate the effects of changes to the composition of IT delivery methods within the banks.

3.3 Justification for the Approach

This study is based on a five year longitudinal case study of two banks in the AFSI and the risks associated with IT multi-sourcing. It also analysed if the current risk and governance frameworks published by APRA are firstly used in each bank, and secondly 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 propositions defined in Chapter 1 (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 data 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, themes or propositions are well defined to ensure the research produces relevant output. In order to meet the objectives of a descriptive Masters research project and the time constraint for delivery of a Masters research project it was decided to firstly select a sample that would provide a reasonable percentage of the AFSI population to allow the research results to be used to provide a projection for the whole of the industry. This is an exploratory study that intends to form the foundation for a future PhD causal research project. The author is planning to use the output from this study to build the foundation for a more formal study involving qualification of the information discovered in this study with the decision makers in a larger sample of banks and the regulatory body. The next paragraph covers the quantity and sources for the data collection.

The two banks selected are the first and second largest banks when ranked according to capitalisation that are fully Australian owned and trade primarily in Australia. This study's sample represents approximately 58 percent (AUD$1,160 billion) of market value of the four major banks (AUD$2,000 billion), 43 percent of value managed by ADIs (AUD$2,724 billion) and 24 percent of the financial value managed under AFSI (AUD$4,900 billion). Table 3.7 summarises the sample breakdown based on the figures extracted from for the Australian Trade Commission (2011) for this research project.

Table 3.7 – The Sample Selected from the Total AFSI

Market Segments	AUD$ Billions	AFSI Market Share	Percentage of the 56 ADIs	Percentage of the 4 Major Banks	Notes
AFSI	4,900	100%			Total Population
56 ADI	2,724	56%			Banking Population
4 Major banks	2,000	41%			The Four Pillars
2 Banks	**1,160**	**24%**	**43%**	**58%**	**Sample**

From Table 3.7 it can be seen the sample selected for this Master's research project represents nearly a quarter of the AFSI and 58 percent of the four major banks.

This is an interpretive study, the author has reviewed published data requiring interpretation when aligning the finding to theories and models that are used to explain and build a picture of the current state of multi-sourcing in the banks. In a future PhD study the researcher can use the interpreted data from this study to perform a critical review with the practitioner in the industry.

3.4 Research Procedures

Applying the software QSR NVivo the research used structured queries to search the research documents for evidence of the occurrences of a theme.

The data analysis followed a systematic approach to develop answers to the research questions. Figure 3.2 provides a road map to demonstrate the source of the data. The steps below outline the process used to build the artefacts that inform the foundations of the study and present the findings of this research.

Step 1. From the literature review develop a list of decision theories that explain decisions on selecting a sourcing model. The decision theories and sourcing models are used as the main themes. Then use these themes as the parameters in a structured query in QSR NVivo. Run the queries to find how many times themes such as 'operational risk', 'risk framework', 'material contracts', 'material agreements', 'strategic technology program', 'FTE', 'IT contractors', 'IT service providers', 'IT vendors' are used and in which part of the banks' annual reports and press releases. The procedure for identifying the frequency of the theme and the section in the bank report where the theme occurs is as follows:

i. Use the Query Wizard under the Query menu option
ii. Select the 1st radio button "See where particular terms occur in content"
iii. Type the theme or term to be searched for and use the exact matches criteria option
iv. Press the "Select" button and select the file to be searched
v. Select the second radio button "Add the Query to Project"
vi. Type in the name and description for the query
vii. Press the "Run" option

viii. Open results window and use the reference tab, work through the list of found themes in the file and note occurrences that meet the study criteria
ix. Using the saved query change the file to be search in "iv" above and repeat the process for all files to be searched
x. Finally repeat point "i" through to "ix" for each theme.

Step 2. From the content analysis carried out on the banks' annual reports develop an IT Sourcing Delivery Model similar to the model shown in Figure 2.3 for each bank. This model highlights the complexity of the delivery model/s currently used by each bank. At this stage we also developed an expenditure trend analysis (Table 3.3) from the IT expenditure information extracted from the banks' annual reports

Step 3. Based on the output from steps 1 and 2, develop the first stage of the Risk Profile and Risk Map for each bank. This forms the foundation of the risk model that is applied across CBA and WBC. Samples are shown in Table 3.4 and Table 3.6 previously.

Step 4. From the content analysis of the banks' annual reports we develop a picture of the banks' governance framework employed to manage service providers and risk.

Step 5. From the content analysis on APRA's governance framework, the researcher extracts the elements used to manage risk associated with IT sourcing.

Step 6. Finally, build a 'Consolidated Risk Profile and Map' to show the industry level impact from the findings from the analysis of the banks' data.

3.5 Ethical Considerations

As all the data that was analysed in this Masters dissertation is available in the public domain, the main ethical consideration from the researcher's perspective was to represent an unbiased view of the data. The data extraction and analysis needs to be transparent and repeatable to allow for verification of the methods used and to ensure that the data results are the same if the processes are repeated by another researcher. Also the data used in this study can be used in future studies therefore the data and interpretation must be accurate and show no signs of bias or manipulation.

3.6 Conclusion

This chapter has covered the research approach that was used to collect the data to perform the data analysis that addresses the overarching research problem, propositions and questions. The reader was informed about where the information was gathered from and where it was stored. Next there was a discussion of the method of data analysis used to extract the data needed to build the artefacts that were used to present the results of the data analysis. The author then provided the justification for using this research method and provided details on academic references that support our approach. To meet the timeline and the objective of the Masters research project, the selection of the sample provides a reasonable percentage of the banking sector of the AFSI that would allow the research results to be used to provide a projection for the whole of the industry. The data from the banks, government agencies and the analysis results will be held securely in a QSR NVivo project file for use in future research.

In the next chapter the author will use the methodology outlined in this chapter and guide the reader through the development of the artefacts that were used to answer

the overarching research problem and propositions outlined in chapter one and research questions formulated in Chapter 2.

Chapter 4 Analysis of Data

Chapter Four presents the results of the data discovered during the analysis phase of the research project. Figure 4.1 provides an overview of the structure of this chapter.

4.1 Introduction

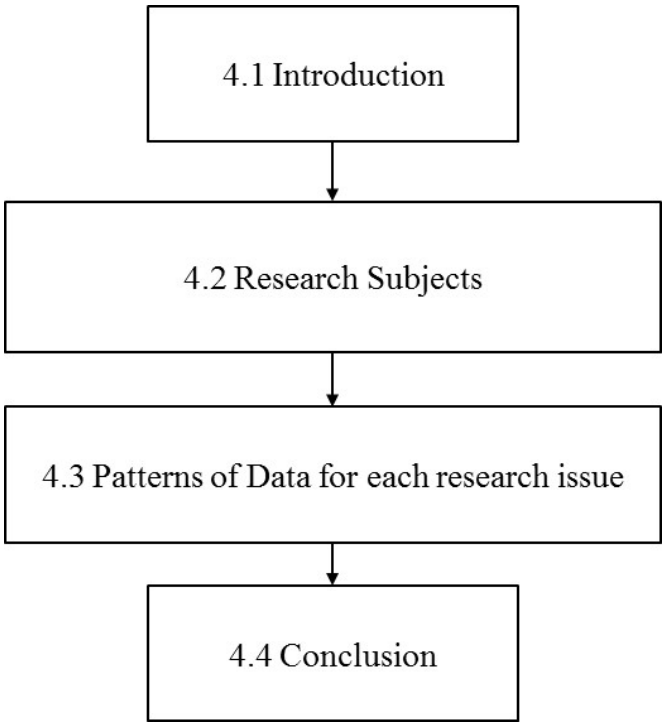
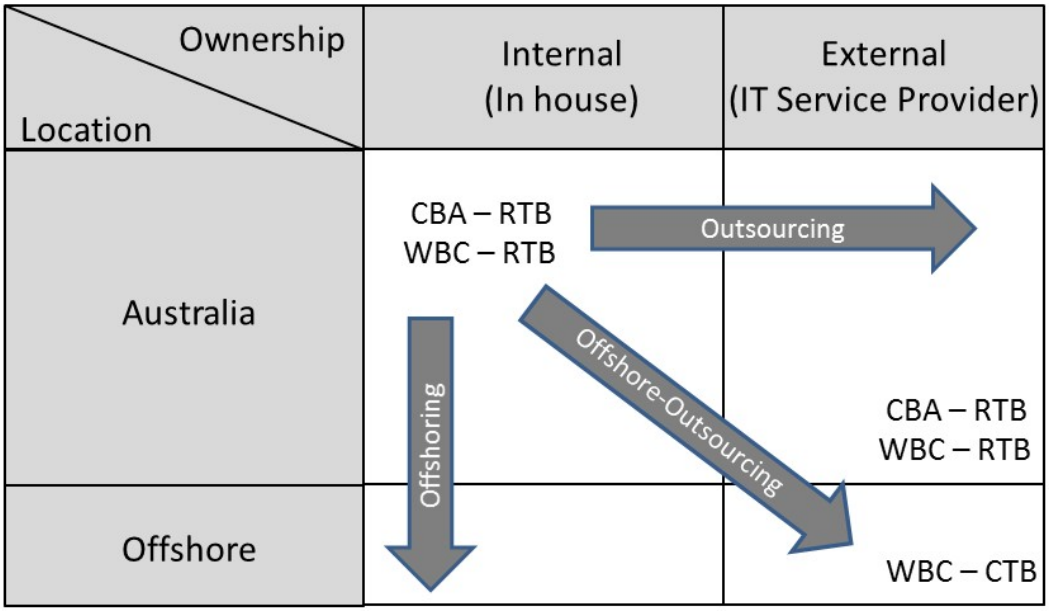


Figure 4.1 – Chapter 4 Structure

Section 4.1 is the introduction to the chapter and lays the foundations and explains the structure of the chapter. Section 4.2 provides the results from the analysis of the data collected from the banks and regulatory bodies. Section 4.3 shows how the results from the analysis address the research problem and propositions outlined in chapter 1 and the research questions introduced in chapter 2. Section 4.4 provides a summary for the chapter along with a link to the next chapter of the dissertation.

4.1.1 High Level IT Sourcing Landscape Across the Banks

The diagram shown in Figure 2.3 was used by Kirkegaard (2008) to demonstrate the different service delivery models. Figure 4.2, based on Kirkegaard's model, provides a high level view of the banks' IT delivery landscape today from an IT service delivery perspective.



Legend:

RTB – Run the bank IT services are core banking needed to meet customer and regulatory commitments.

CTB – Change the bank IT services are the IT activities associated with transformation or modernisation of the banking systems.

Figure 4.2 – High Level Sourcing Landscape

Figure 4.2 demonstrates that Run the Bank (RTB) IT services are dominated by outsourcing services. RTB IT services are predominately infrastructure services, data centres, application maintenance and testing, networks, end user computing and operational support for core banking systems that are managed and run from the data centres. The Change the Bank (CTB) services show a mix of in-house, offshoring and offshore-outsourcing. The CTB services would include application development, testing and project delivery. CTB services provide the banks with a vehicle to deliver innovation and transformation, whereas the RTB services provide the operational stability needed to maintain the bank's core banking services. It should be recognised that the transformational programs instigated under CTB IT Services transition to RTB IT Services once the program or project is completed and the system is passed to the IT operations team to manage.

Both the RTB and CTB have different operational risks associated with them. In an article that investigated the challenges banks have balancing the risks associated with CTB and RTB the findings aligned with the detail outlined in the previous paragraph (Mestchian 2012).

The sourcing landscape provided in Table 4.1 is based on the high level view of the banks' sourcing strategies (shown in Figure 4.2) and breaks it down further into specific IT services delivered by the banks' IT business units.

Table 4.1 – IT Services, Delivery Sourcing Profiles of the Banks

	CBA Method of Delivery				WBC Method of Delivery			
	Outsource	Outsource Offshore	Offshore	In-house	Outsource	Outsource Offshore	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	☑			☑				☑

Table 4.1 shows that both banks use a mix of outsourcing, offshore-outsourcing and in-house delivery methods to deliver different components of their IT services. It can be seen from Table 4.1 that both banks use outsourcing to deliver the majority of their IT infrastructure services. The mix of delivery methods becomes more complex in the IT application services area. In the enterprise services space the banks have mostly kept these in-house especially the architecture services.

The reasons behind why the banks made these decisions will be investigated in a future study when interviews will be carried out with the banks' IT and commercial senior management teams. This clearly shows that the delivery model in each bank is complex and each bank has selected a different configuration to deliver IT services at a components level. This indicates that each bank has a potentially different risk profile due to the different combination of IT delivery models selected to deliver IT services to the banks' business units.

4.2 Research Subjects

Based on the data extracted from APRA's prudential regulations relating to the governance of BCM, outsourcing and operational risk (APRA 2005, 2006, 2013a). The information extracted from the prudential regulations was used to build the risk framework, risk profile and risk maps for CBA and WBC. The CBA and WBC risk artefacts were used to provide a consolidated risk profile that forms part of the information used to address research question three outline in Chapter 2 section 2.7.

From the banks' annual reports (CBA 2009, 2010, 2011b, 2012, 2013; WBC 2009, 2010a, 2011, 2012, 2013) we extracted, analysed and presented the IT services

sourcing trend analysis both from a financial and function perspective, this shows how the current sourcing mix was derived. This information is used to assist in the formulation of the answers to research question one outlined in Chapter 2 section 2.7.

A combination of the results from the analysis of the APRA data and the data from the bank's annual reports is used to build a risk profile and risk map that shows how the multi-sourcing mix impacted the risk profile for each bank. This information will be used to address research questions three outline in Chapter 2 section 2.7 of this thesis. Table 4.2 provides descriptions of the risk profile components used in the risk profiles for CBA, WBC and combined risk profiles. All three risk profiles use the same risk components list that derived from the categories that the banks use to report on risk in their annual reports.

Table 4.2 – Risk Component Descriptions

Risk Component	Brief Explanation
Governance and Risk Management	Failure in governance or risk management, the less structured the governance and risk organisation the higher the probability of failure.
Skills and Knowledge Management	The lower the knowledge management system and training to maintain employee skill the higher the probability of a failure occurring.
Companies fit and Alignment	Cultural differences have an impact on success, it can vary from an uncooperative situation that requires tight management using the commercial framework to a cooperative relationship that provides a partnership approach. The more cooperative the company alignment the lower the probability of failure.
Quality Management	The less disciplined the quality control (ITIL, CMMi etc.) management processes and procedures the higher the probability of a failure therefore the higher the risk probability rating.
Sovereign Risk / On-Going concern	The higher the risk of civil disturbance of country the higher the risk probability. This measurement can even go a low a city or state within a specific country.
Offshore facilities (capacity for growth)	This risk is based not only on a service provider's ability to expand the service centre in another country but also their ability to staff it with the right resources to provide the right level of service.
Commercial	The more complex the commercial framework or the lack of a commercial framework will increase the probability to realise this risk.
Sustainability	This risk takes account of the service providers' maturity and their ability to maintain their position in the market. It also factors in the complexity of the solutions and how well knowledge management is managed between the bank and the service provider.
Critical projects	The high the criticality of the projects allocated to a service provider the high the risk because the higher the criticality of the project the more likely it is part of the core intellectual property of the bank and failure will have a higher impact.
Data Leakage and Confidentiality	Security of data being access from an overseas location or being transmitted to an overseas location. This include documentation as well as customer data.
Service Provider Mix	The higher the number of service provider the higher the probability and impact of this risk component.

4.2.1 Regulatory Governance and Risk Frameworks

The BCBS produced an 'Outsourcing in Financial Services' report in February 2005 that included several case studies on aspects and challenges of outsourcing in the financial services industry (Basel Committee on Banking Supervision 2005). Figure 4.3 reproduces one of the case studies published in the report. The case study

was carried out by the Australian regulator (APRA) into outsourcing within the Australian banking industry.

Case Study 2: Australian regulator investigates bank outsourcing

Australian banks have outsourced activities including information technology, credit card services, procurement, cheque and other electronic clearing services, mortgage processing and payroll, amongst others. This raises questions about privacy of customer information and the financial and reputational risks to the banks if a service provider experiences problems or cannot go on providing.

In January 2002, the Australian Prudential Regulation Authority (APRA) completed a targeted review of bank outsourcing and introduced detailed prudential standards from 1 July 2002.

APRA found that outsourcing arrangements were managed in a number of ways. Larger institutions generally had a dedicated outsourcing unit responsible for ensuring the institution's outsourcing policy is applied consistently. However, a number of institutions delegated responsibility for outsourcing to business units. In these cases, there was no guarantee that risks would be appropriately identified and assessed, and there was no central point for monitoring outsourcing arrangements.

Fewer than one-third of institutions surveyed had a formal policy on outsourcing. In most cases banks were able to articulate the types of activities that could be outsourced or the reasons for outsourcing an activity, but this had not been formalised.

Source: Basel Committee on Banking Supervision: Outsourcing in Financial Services, February 2005, P. 26

Figure 4.3 – Basel Committee - Case Study Summary

The case study results shown in Figure 4.3 clearly highlights that less than one-third of banks had a clear policy on outsourcing. It found that the governance models and risk management framework were inconsistently implemented and managed across the sample. This situation led APRA to develop and introduce the first prudential standard in July 2002 and revise it in 2006 (APRA 2006) to clearly articulate the AFSI policy and guidelines for outsourcing. With a standard in place for outsourcing does the AFSI need a new or separate policy to cover offshore-outsourcing or are the risks the same?

Issue 1: Does APRA treat the three sourcing delivery models the same as suggested by the prudential standards APRA (2006) and APRA (2005)?

Response 1: APRA does not make any distinction between outsourcing, offshore-outsourcing and offshoring as demonstrated in APS 231 which clearly states in point 9 in the interpretation section on page 2 that:

"For the purposes of this Prudential Standard, ***offshoring*** *means the outsourcing by an ADI of a material business activity associated with its Australian*

business to a service provider (including a related body corporate) where the outsourced activity is to be conducted outside Australia".

The Basel Committee's paper on guidelines on outsourcing in the financial services makes reference to the trend in offshoring within financial services (Basel Committee on Banking Supervision 2005). The Basel Committee set up a special interest group (SIG) which included the Chairman of APRA as a member. The SIG was tasked to draw up guidelines for prudential supervisors on implementing and governing operational risk. The SIG's paper makes no reference to offshoring but does draw attention to the operational risk management associated with outsourcing (Basel Committee on Banking Supervision 2011b):

"Outsourcing is the use of a third party – either an affiliate within a corporate group or an unaffiliated external entity – to perform activities on behalf of the bank. Outsourcing can involve transaction processing or business processes. While outsourcing can help manage costs, provide expertise, expand product offerings, and improve services, it also introduces risks that management should address. The Board and senior management are responsible for understanding the operational risks associated with outsourcing arrangements and ensuring that effective risk management policies and practices are in place to manage the risk in outsourcing activities. Outsourcing policies and risk management activities should encompass:

(a) procedures for determining whether and how activities can be outsourced;
(b) processes for conducting due diligence in the selection of potential service providers;
(c) sound structuring of the outsourcing arrangement, including ownership and confidentiality of data, as well as termination rights;
(d) programmes for managing and monitoring the risks associated with the outsourcing arrangement, including the financial condition of the service provider;
(e) establishment of an effective control environment at the bank and the service provider;
(f) development of viable contingency plans; and
(g) execution of comprehensive contracts and/or service level agreements with a clear allocation of responsibilities between the outsourcing provider and the bank" (Basel Committee on Banking Supervision 2011b, p. 16).

Issue 2: What risk framework is used by APRA to govern the banks?

Response 2: The risk framework for managing operational risk using the advanced measurement approach (AMA) has been documented in a prudential standard APS 115 and both CBA and WBC have approval to use this standard to measure and manage operational risk (APRA 2013a).

Issue 3: Does APRA measure changes to the industry risk profile with the banks' move to offshore-outsourcing more of their IT services?

Response 3: There was no evidence obtained from the analysis of the data that APRA treats the risk profile of the AFSI as a whole any differently in relation to the percentage of services a bank offshore-outsources. APRA leave it to the bank to establish the capital adequacy for its sourcing strategy based on AMA (APRA 2013a). It is also evident from the papers produced by the Basel Committee that the Basel Committee and Basel SIGs do not differentiate between the different IT delivery models (Basel Committee on Banking Supervision 2011b).

4.2.2 Findings from CBA IT Sourcing Strategy Analysis

The CBA was founded under the Commonwealth Bank Act in 1911 and commenced operations in 1912, empowered to conduct both savings and general banking business. The CBA Group is made up of Commonwealth Bank of Australia, CommInsur, Bankwest, CommSec, Colonial First State, Colonial First State Global Asset Management and ASB and Sovereign in New Zealand. CBA has 44,969 full time equivalent (FTE) employees, a total revenue of $21,499 million with operating expenses of $9,605 million in 2013 (CBA 2013).

The history of CBA's IT sourcing strategy commenced in 1997 when CBA used a co-sourcing approach through its outsourcing agreement with Electronic Data Systems (EDS) for all IT Services managed under a single Master Services Agreement (MSA) (CBA 1997). Over the following 10 years it moved to a multi-sourcing outsourcing model under separate MSAs aligned to IT functions, for example: mainframe support services, mid-range services, desktop services and ATM services etc. Mid-2000s the bank engaged service providers based in India for IT transformation programs, primarily for application development and maintenance (ADM) services (CBA 2009, 2010, 2011b).

One strategy CBA have never wavered from since the 1990 was that they do not send Australian jobs offshore (Newman 2013; Tait 2012). No evidence has been discovered that directly links activities carried out by CBA resulting in any CBA role being passed to a service provider who then delivered this service from an offshore delivery centre. CBA leadership has also made it clear they contract to buy services from IT service providers and it is the IT service providers' decision on the most effective model to deliver IT services at the cost and quality agreed in the commercial agreement. CBA do require all IT service providers to adhere to the security and risk compliance guidelines for the delivery of the IT services as contracted.

Stage 1 of this study involved extracting from the CBA annual reports information on the IT services for which CBA published information and details of the delivery model employed. Table 4.3 was developed to summarise the data extracted using queries in QSR NVivo.

Table 4.3 – CBA IT Sourcing Landscape

CBA	Method of Delivery			
	Outsource	Outsource Offshore	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 IT sourcing landscape in Table 4.3 demonstrates CBA uses a complex mix of outsourcing, and in-house delivery methods to deliver different components of their IT services (IT multi-sourcing). It can be seen from Table 4.3 that the bank 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 kept most of its enterprise services in-house as this is key IP for the bank's IT strategy. With the bank's policy on not declaring where their IT services are delivered from. It could be inferred that delivery centres outside Australia could be used as each of the Indian based IT service provider contracted by CBA have the capability to deliver some of the services to CBA from an offshore location.

In Stage 2 the author has compiled the CBA sourcing trend analysis as summarised in Table 4.4. This table provides key data of the bank's staffing and IT Service Provision and was extracted from CBA Annual Reports to inform the next stage of the analysis (CBA 2009, 2010, 2011b, 2012, 2013).

Table 4.4 – CBA IT Sourcing Trend 2009-2013

$ are in millions of Australian Dollars					
CBA	**2009**	**2010**	**2011**	**2012**	**2013**
Full-Time Equivalent employees (FTE)	44,218	45,025	46,060	44,844	44,969
Australian Agencies (Contract Employees)	3,859	3,884	3,795	3,818	3,764
Total Workforce	**48,077**	**48,909**	**49,855**	**48,662**	**48,733**
FTE Expenses					
Share-based compensation	$125	$130	$156	$185	$192
Superannuation - defined contribution plans	$44	$48	$48	$42	$58
Superannuation - defined benefit plan	$14	$103	$137	$168	$204
Provisions for employee entitlements	$88	$58	$120	$101	$96
Payroll tax	$188	$202	$213	$213	$223
Fringe benefits tax	$36	$40	$38	$35	$35
Other staff expenses	$94	$157	$60	$67	$90
Total FTE expenses	**$589**	**$738**	**$772**	**$811**	**$898**
Information Technology Services					
Application, maintenance and development	$167	$209	$324	$322	$439
Data processing	$202	$227	$267	$241	$236
Desktop	$141	$141	$120	$105	$100
Communications	$179	$199	$221	$226	$202
Amortisation of software assets	$122	$178	$183	$183	$245
IT equipment depreciation	$62	$75	$78	$82	$77
Total information technology services	**$873**	**$1,029**	**$1,193**	**$1,159**	**$1,299**

The CBA IT sourcing trend shown in Table 4.4 has three main sections: the first section is the workforce, with a split between FTE and domestic contract staff. CBA only discloses the overall costs associated with the FTE human resources which is shown in the second section.

The third section in Table 4.4 is the Information Technology Services costs. These services are funded independently of resources and aligning this to a IT services commercial framework it can be construed that at least the following are outsourced services: Application maintenance and development; Data processing; and Desktop and Communications. The author cannot, with any certainty, ascertain the percentage of which of these services may be delivered from an IT delivery centre outside Australia. In its annual reports from 2009 until 2011 the CBA published details on long term contracts that had a material impact on the bank. In the 2009 to 2011 annual reports the following statement was included in the long term contract section that related to sourcing of technology services:

"*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*" (CBA 2009, 2010, 2011b)

This statement indicates a move from a dedicated IT outsourcing service provider providing all technology service to an IT multi-vendor model with the capabilities for IT multi-sourcing. Two of the new IT service providers are based in India with capabilities to deliver IT services from an offshore location. Also IBM Australia Ltd has a large offshoring capability in India via IBM India that has the capability to provide services into Australian companies as IBM Australia provides to other companies in Australia.

In the 2012 and 2013 annual reports this statement is omitted with no explanation why this information has been excluded.

With this information as background, the graph shown in Figure 4.4 articulates the changes in CBA's technology spending from 2009 until 2012 for each of the following technology areas: Application, maintenance and development, Data processing, Desktop and Communications. These four areas fit under the umbrella of services listed in the information technology services section of Table 4.4 that can be outsourced, offshore-outsourced, offshored or performed in-house.

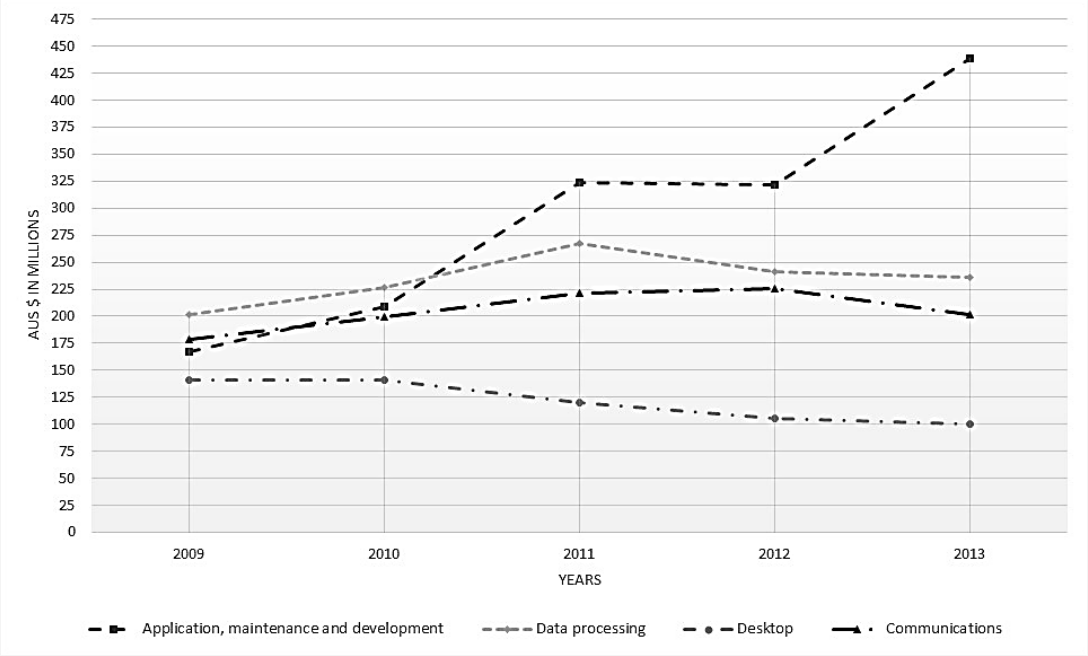


Figure 4.4 – CBA Technology Services Spend from 2009 to 2013

As can be seen in Figure 4.4 between 2009 and 2013 CBA's spend on application maintenance and development grew substantially, while the expenditure on the other three lines of service has either remained fairly flat or declined.

In terms of percentage change, Figure 4.5 shows quite a confusing spending pattern.

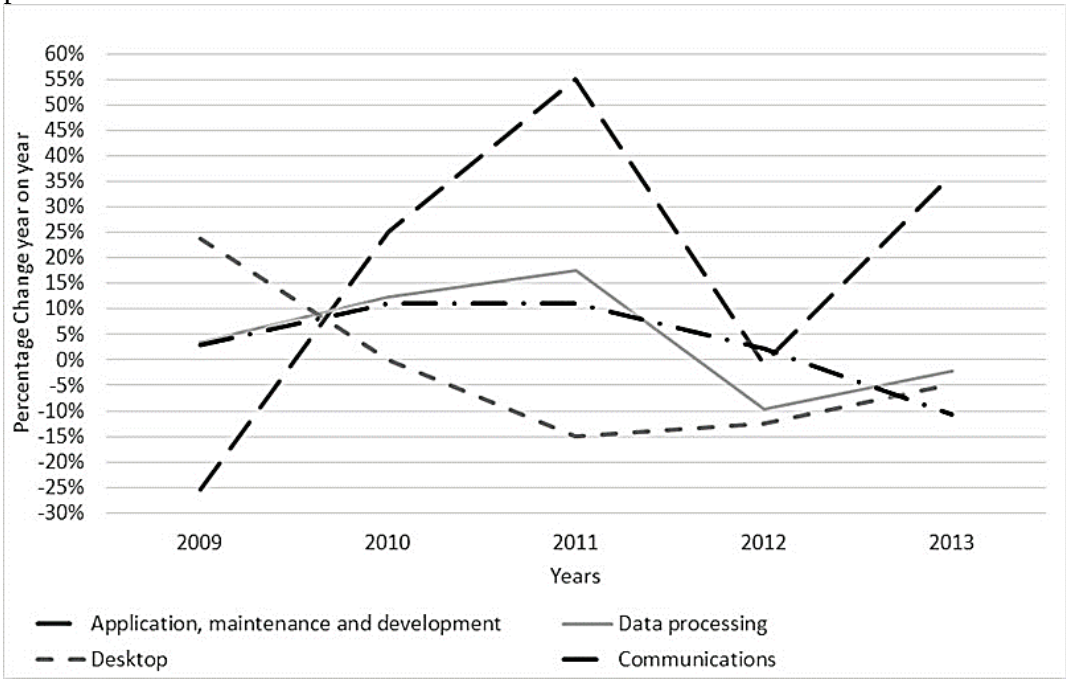


Figure 4.5 – Percentage Change Year on Year CBA IT Spend

The spending on Application, maintenance and development IT services had substantial growth from 2009 through to 2011; then investment dropped in 2012 and was followed by substantial growth in 2013. This is not representative of a normal budgeting pattern for any IT business unit. The spending on Data Processing IT services grew from 2009 through to 2011; then substantially contracted for 2012 and 2013, again the budgeting pattern is not clear. The spending on Desktop IT services had no growth between 2009 and 2010 then a reduction in spending from 2011 through to 2013. Finally, spending on Communications IT services did not change between 2010 and 2011 and the spending pattern declined from 2012 to 2013. The author will explore some of the reasons for these unusual patterns in IT spending by CBA in Chapter 5.

4.2.2.1 CBA – View of Risk and Governance

The two areas that the analysis focused on were the risk framework used within the bank and the governance framework and how these two frameworks coexist within the bank. Analysing these two frameworks together provides the researcher with the ability to check if these two frameworks together align with the APRA risk and governance framework governed by the prudential standards (APRA 2013a).

4.2.2.1.1 CBA - Operational Risk Framework

As part of CBA aligning to the APRA risk framework and using AMA to measure operational risk, CBA published the following definition of operational risk. This operational risk definition has remained unchanged during the analysis timeframe 2009 to 2013:

"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.

The Group's Operational Risk Management Framework (ORMF) supports the achievement of its financial and business goals. The following objectives have been approved by the Risk Committee:

- *Maintenance of an effective internal control environment and system of internal control;*
- *Demonstration of effective governance, including a consistent approach to operational risk management across the Group;*
- *Transparency, escalation and resolution of risk and control incidents and issues; and*
- *Making decisions based upon an informed risk-return analysis and appropriate standards of professional practice.*

The Group measures operational risk using an APRA approved Advanced Measurement Approach capital model which is integrated into the ORMF. The inputs include scenario analysis, loss data and risk indicators" (CBA 2013).

It can be seen from CBA's operational risk definition that technology risk is included as part of the definition which is in line with both the APRA and BCBS definitions.

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 through to the Board using the CBA three line of defence Governance framework which is detailed in the next three paragraphs.

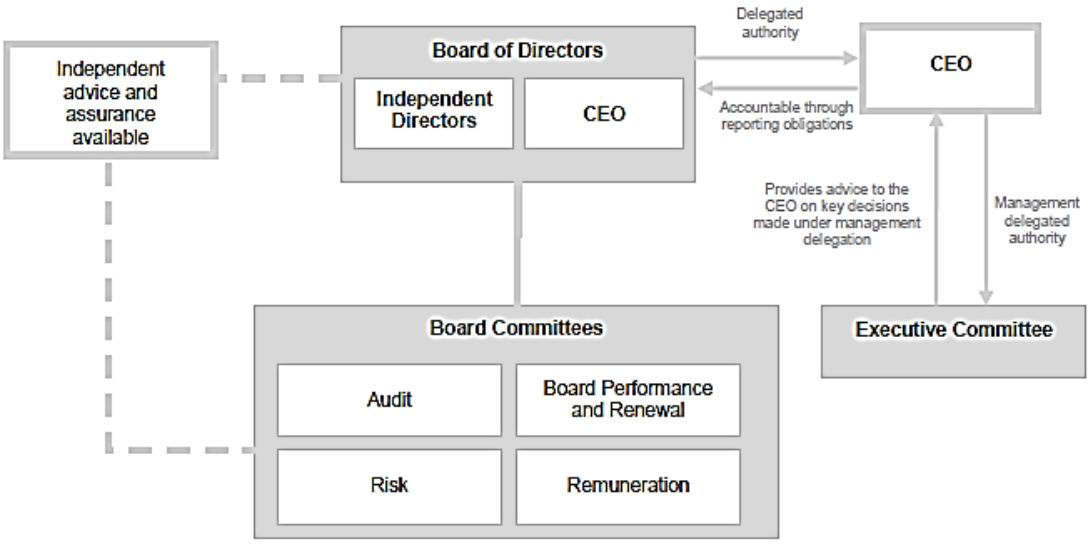
The first line of risk defence is embedded in the business unit and forms part of the business unit management function. At this level, the business unit manager is responsible for managing risk within the corporate risk management framework and risk appetite of the business unit.

The second line of risk defence is the risk management business unit that is tasked with expertise and governance of the risk management function within the corporate risk and governance framework. The risk management team also have accountability for approving delegation of authority and the risk exposure proposed by the business unit.

The third and final line of risk defence is the group audit and assurance business unit: it provides independent oversight of adherence to the risk and governance frameworks across all business units.

4.2.2.2 CBA – Governance Framework

As shown in Figure 4.6, the corporate governance structure is setup to separate the non-executive members (Independent Directors) from the Executive of the CBA.



Source: Commonwealth Bank of Australia, *Annual Report 2013*, p. 36.

Figure 4.6 – CBA Corporate Governance Structure

This structure provides independent governance of the bank without interference from the day to day running 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 and reports to the Board and heads the executive of the bank. The Board has several committees that oversee the running of the bank: audit; Board performance and renewal; risk; and remuneration. 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.

4.2.2.3 CBA – Risk Position from the Analysis

The data presented in Table 4.5 was extracted from the data analysis carried out on the CBA's annual reports (CBA 2009, 2010, 2011b, 2012, 2013). The information gathered was used to establish the parameters that allowed the research to calculate the impact rating shown in Table 4.6 for each component of risk that was identified as needing to be managed as part of the bank's sourcing strategy. These impact ratings can be used in a future study as part of an objective questionnaire that can be used as part of a structured interview.

Table 4.5 – CBA Impact Rating Measurement

Component of Risk Management	Rating	Evidence
Governance and Risk Management	Very High	CBA's governance and risk management is untested except for their BCP component. The potential risk impact is very high until scenario or simulation models can show the governance and risk management framework provide sufficient protection.
Skills and Knowledge Management	Very High	16 major IT Projects
Companies fit and Alignment	High	A published vendor selection process exists and has been in use since 2011 but no results have been published. (High = Published but in use for less than 3 years.)
Quality Management	Medium	8 years, introduced as part of the renewal of mid-range and storage services with EDS
Sovereign Risk / On-Going concern	Low	No offshore delivery centres
Offshore facilities (capacity for growth)	Low	No offshore delivery centres
Commercial	Very High	5 major IT services contract
Sustainability	Low	100% in-house delivery of IT services
Critical projects	Very High	16 major IT projects
Data Leakage and Confidentiality	Low	100% onshore data storage and access only from CBA controlled premises
Service Provider Mix	High	3 IT service providers

Using the research approach outlined in Section 3.2 to develop the CBA risk profile, Table 4.6 shows the results from the data analysis from CBA.

Table 4.6 – 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 4.7 shows the risks map based on the impact and probability results shown in Table 4.6.

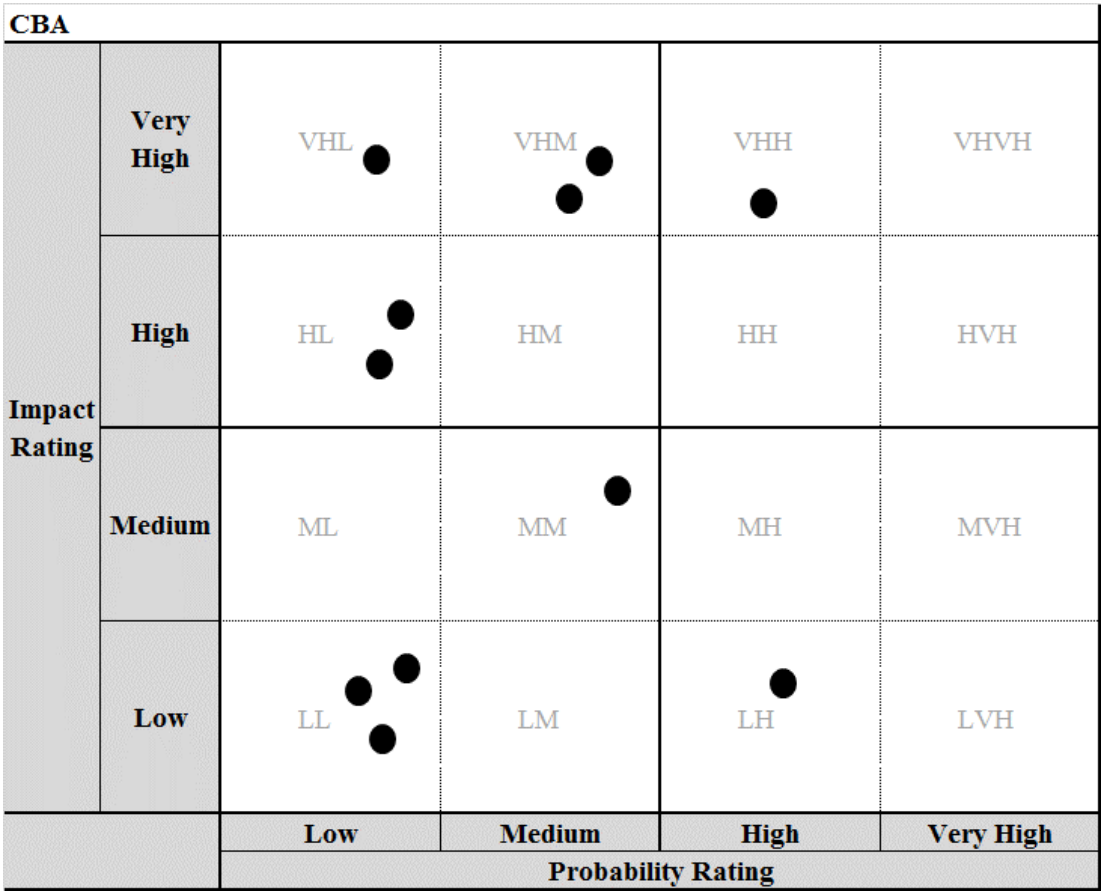


Figure 4.7 – CBA Risk Map

Each black dot on the map represents one risk category from the risks listed in the risk profile (Table 4.6). For the analysis in this study this map provides a simple picture of the risk spread. The author has not associated mitigation activities to these

risks as there is no need to over-complicate the picture by labelling each risk dot. In Figure 4.7 it is clear that the risks identified in Table 4.6 are evenly spread across three of the four quadrants. This indicates that the impact to the bank for the majority of the risks would be fairly high but the probability of the risk being realised is fairly low. This does not mean the bank can ignore the risks but with the right level of management attention and monitoring the risks are manageable. Neither the risk map, nor the risk profile, show what, if any, mitigation programs are in place to address the risks.

4.2.3 Findings from WBC IT Sourcing Strategy Analysis

WBC was founded in 1817 and is the second largest bank in Australia (as at 30th September 2013). WBC is comprised of the parent company Westpac Retail and Business Bank, Westpac Institutional Bank, St George Bank, RAMS, Westpac New Zealand, Bank of Melbourne, Bank of South Australia and BT Financial Group. WBC has 35,597 full time equivalent (FTE) employees, a total revenue of $18,833 million with operating expenses of $7,710 million (WBC 2013).

WBC outsourced its IT infrastructure services to IBM Global Services Australia (IBM GSA) in the late 1990s and retained its ADM services in-house. WBC employed a high number of consultancy companies and local contractors to meet fluctuations in demand within ADM services. In 2010 WBC decided to move ADM services to a multi-vendor offshore-outsourcing model. WBC selected four service providers to provide transformational ADM programs under the strategic improvement priorities (SIP) programs and also the support and maintenance of its current application and systems portfolio.

The SIP initiative was a selection of 13 major programs that would enable WBC to modernise all aspects of the bank. The SIPs changed everything from the layout of the branches, the technology in the branches, how customers experienced and conducted business through to the tools and infrastructure used to deliver new systems. The SIP programs were all scheduled for completion by the year 2017 to coincide with the 200th anniversary of the founding of WBC as the Bank of New South Wales.

The four selected service providers comprised three Indian based service providers (Infosys, Tata Consulting Services (TCS), and Wipro) and one global service provider (IBM) that also acts as outsourced IT infrastructure service provider to WBC.

Table 4.7 – WBC IT Sourcing Landscape

WBC	Method of Delivery			
	Outsource	Outsource Offshore	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 in Table 4.7 demonstrates how WBC uses a complex mix of outsourcing, offshore-outsourcing and in-house delivery methods for different components of their IT services (IT multi-sourcing). It can be seen from Table 4.7 that the bank uses outsourcing to deliver the majority of IT infrastructure services. The mix of delivery methods becomes more complex in the application services business unit. WBC has kept enterprise services in-house as this is key IP for the bank's IT strategy.

In Stage 2 the author has compiled the WBC sourcing trend analysis as summarised in Table 4.8. This table provides key data of the bank's staffing and IT Service Provision and was extracted from WBC Annual Reports to inform the next stage of the analysis (WBC 2009, 2010a, 2011, 2012, 2013).

Table 4.8 – WBC IT Sourcing Trend 2009-2013

$ are in millions of Australian Dollars					
WBC	**2009**	**2010**	**2011**	**2012**	**2013**
WBC FTE	37,032	38,962	37,806	35,675	35,597
Percentage change – WBC FTE year on year		5%	-3%	-6%	0%
WBC IT FTE	8,530	11,174	11,600	10,058	10,163
Percentage change – IT FTE year on year		24%	4%	-15%	1%
Split of WBC IT FTE to WBC FTE	23%	29%	31%	28%	29%
FTE Costs for The Bank Group					
Total salaries and other staff expenses	$3,806	$3,990	$4,055	$4,258	$4,287
Year on Year Change – WBC FTE Spend		$184	$65	$203	$29
Average Cost per WBC FTE	$103	$102	$107	$119	$120
Internal IT Services Costs					
Technology – Property, plant and equipment	$666	$707	$610	$574	$569
Calculated Cost of IT FTE	$877	$1,144	$1,244	$1,200	$1,224
Year on Year Change – IT FTE Cost		$268	$100	-$44	$23
Externally IT Services					
IT Services Outsourcing spend	$514	$526	$592	$620	$587
Incremental Change – IT Outsourcing Spend		$12	$66	$28	-$33
IT Services Offshore spend	$249	$280	$254	$278	$350
Year on Year Change – IT Offshore-outsourcing Spend		$31	-$26	$24	$72
Total Cost to Deliver IT Services	**$2,306**	**$2,657**	**$2,700**	**$2,672**	**$2,730**
Incremental Change Total IT Services Costs		$352	$43	-$28	$57
Total Spend on External IT Services	**$763**	**$806**	**$846**	**$898**	**$937**
Percentage spend – IT Offshore-outsourcing Services	67%	65%	70%	69%	63%
Percentage spend – IT Outsourcing Services	33%	35%	30%	31%	37%

To provide more clarity to the information in Table 4.8 we provide a set of definitions:

- *WBC – Westpac Banking Group:* all the divisions and companies under the parent company.
- *FTE* – Full Time Equivalent: full-time, pro-rata part-time, temporary and domestic contract staff.

In interpreting this indicator, it is important to note that unlike most organisations, WBC includes domestic contract staff in FTE headcount.

- *IT or IT Services:* IT infrastructure maintenance & support, data centre, desktop, network, telecommunication and application development & maintenance (ADM) services, excluding business processes that manage the bank's customer business.
- *IT Outsourcing:* IT Services delivered and managed by an IT Service Provider from within Australia. These are managed under an outsourcing commercial agreement based on defined IT Services.
- *IT Offshore-outsourcing*: IT Services delivered and managed by an IT Service Provider from outside Australia. These are managed under zero volume commercial agreements and services can be delivered as resources or services.

WBC entered into three major IT services agreements between 2010 and 2013 that influenced the composition of the IT services delivery model with the introduction of external IT service providers with offshore delivery capabilities. These agreements have had a direct impact in the mix of IT outsourcing and IT offshore-outsourcing services at WBC:

1. On 25 June 2012, WBC commenced a five year agreement with Tata Consultancy Services (India) to provide maintenance and development support within the information systems area of technology. In November 2012, WBC commenced an additional five year agreement with Tata Consultancy Services to provide maintenance and development support within the customer self service area of technology. This is an offshore-outsourcing agreement for ADM services. It was driven primarily by the major transformation program the bank is undertaking.
2. On 25 June 2012, WBC commenced a five year agreement with Infosys Technologies Limited (India) to provide maintenance and development support within the testing and corporate systems areas of technology. In November 2012, WBC commenced an additional five year agreement with Infosys Technologies Limited to provide maintenance and development support within the group customer Master and customer assisted services areas of technology. This is an offshore-outsourcing agreement for ADM services, driven primarily by the major transformation program the bank is undertaking.
3. On 30 September 2013, WBC entered into an agreement with IBM Australia Limited to provide project delivery resources from India specific for Integrated Migration and Transformation Program (IMTP) requirements. This is an offshore-outsourcing agreement for ADM services additional to the outsourcing agreement with IBM Australia Limited. This agreement was driven primarily by the major SIP transformation programs the bank is undertaking.

It is important to note that during the time period under review, WBC introduced the SIP programs to transform and modernise the bank. The SIP programs impact all areas of the bank, not only the IT business unit.

Based on the data extracted, analysed and presented in tabular format in Table 4.8, Figure 4.8 shows the major influences on WBC FTE and WBC IT FTE staff numbers over the 2009 to 2013 period.

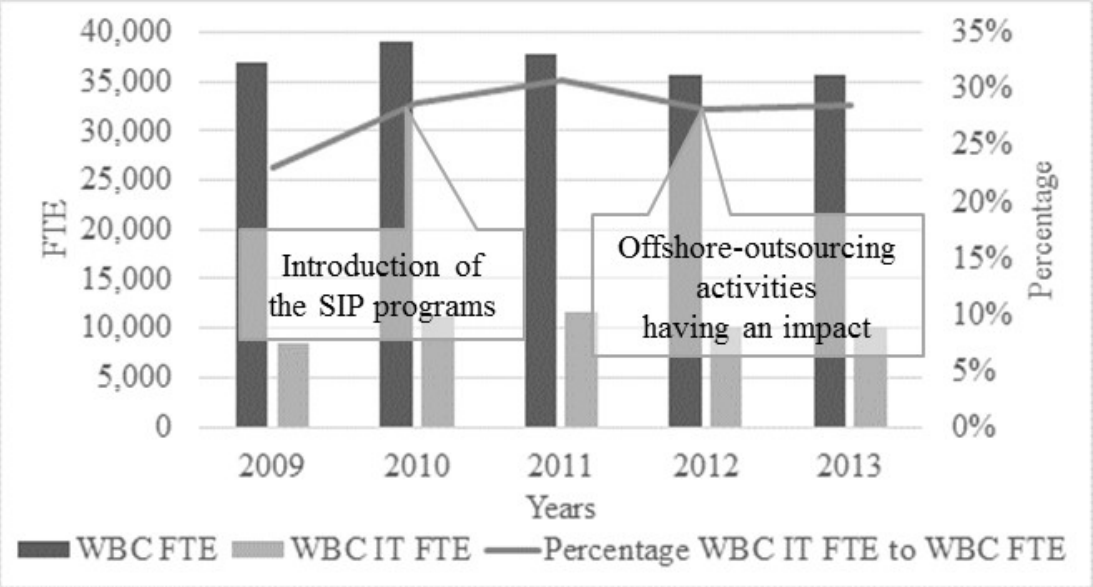


Figure 4.8 – Comparison of WBC Bank FTE to WBC IT FTE Over 5 Years

Firstly and most importantly the introduction of the SIP programs impacted all areas of the bank, not just the IT business unit. Secondly, even with the increase in demand for IT FTE due to the SIP programs, the Sourcing SIP delivered FTE savings in 2012 by implementing offshore-outsourcing as one of its sourcing strategies.

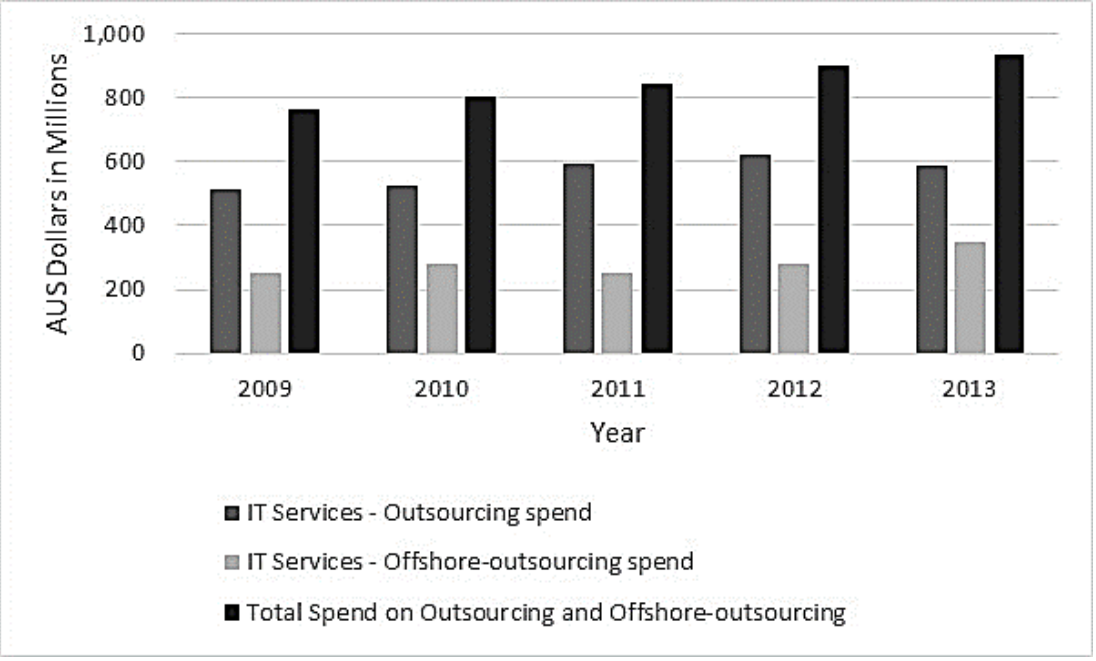


Figure 4.9 – Analysis of IT Services Spend

From Figure 4.9 (based on Table 4.8) we can see that the major influences on WBC IT outsourcing activities were firstly driven by the introduction of the SIP programs in 2010 that dramatically increased the spend due to infrastructure improvement SIP programs that relied on the IT outsourced service provider. The decrease in 2013 was as a result of bringing outsourced IT services back in-house that previously were performed by the IT service provider or were duplicated by the IT outsourcer and WBC internal IT infrastructure services business units.

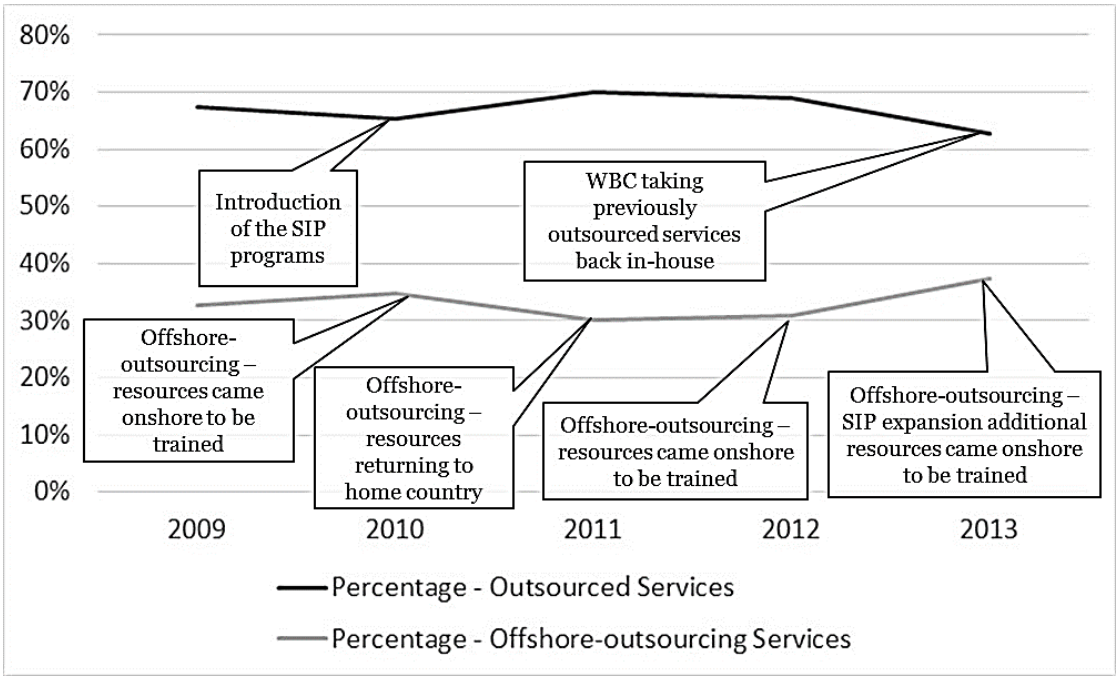


Figure 4.10 – Influences on Total External IT Services Spend

Based on Table 4.8, Figure 4.10 shows that the major influences on WBC IT offshore-outsourcing were for a variety of reasons. The process of introducing IT offshore-outsourcing involved the following. Firstly, the offshore personnel come onshore to train and perform knowledge transfer (KT) from the current WBC FTE staff. Whilst the staff are onshore, WBC pays a higher daily rate for the personnel, at a rate very close to that charged by local contractors. Once the training and KT is complete, the offshore personnel return to home base and start work from the offshore delivery centre. From this point on, WBC then pays a much lower offshore rate for the same human resource performing the same duties. It needs to be recognised that the data in Figure 4.10 does not reflect separately the growth in demand that was filled by using offshore resources rather than local contractors or the outsourcer. The important period in Figure 4.10 to focus on is 2010 to 2011. The KT from the current IT contract workforce was completed and the service provider moved the offshore resources back to home base. This resulted in a substantial decrease in cost to WBC. The increase in spend after this is due purely to growth in demand being fulfilled through this model rather than in-house or domestic outsourcing.

4.2.3.1 WBC – View of Risk and Governance

As part of WBC aligning to the APRA risk framework and using AMA to measure operational risk, WBC published the following definition for operational risk. This operational risk definition is aligned with the definition provided in the APRA risk framework and guidelines APRA (2013a) and has remained unchanged during the analysis timeframe 2009 to 2013.

WBC - Definition of Operational Risk:

> "*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, p. 37).

WBC also provides a definition of Technology Risk, developed to enable it to measure technology risk as a separate monitoring and reporting track outside of operational risk during the massive changes caused by the SIP initiatives. APRA and Basel embed technology risk as part of operational risk. It should be recognised that the technology risk definition is independent of how services are sourced and sourcing does not have a risk definition.

WBC - Definition of Technology Risk:

> *"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, p. 112).

To summarise, WBC's risk management framework and corporate governance model provide comprehensive management and governance of risk within the bank as shown in Figure 4.11 (WBC 2009, p. 37).

Source: WBC 2013 Annual Report, p. 37

Figure 4.11 – WBC's Risk Defence Model

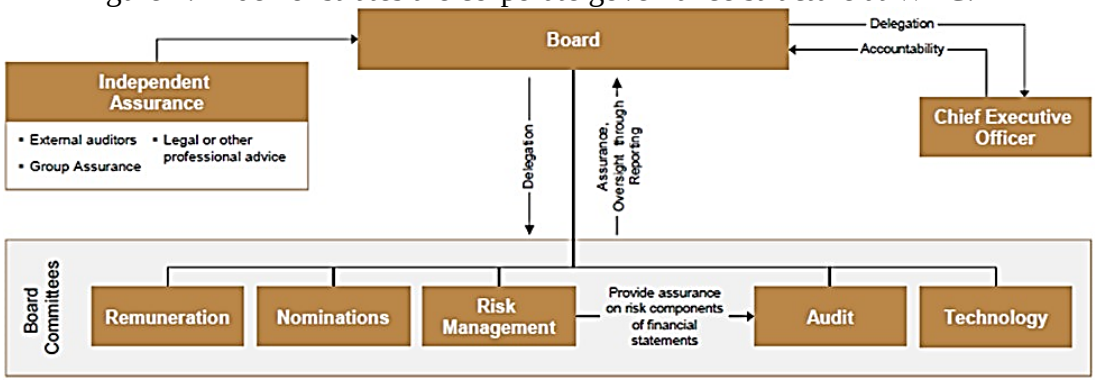
The WBC Risk Defence Model will be reviewed in section 5.3 of Chapter 5 against the regulator's model enable us to evaluate and discuss in more detail whether

this model, based on prudential risk management, is sufficient to manage the risks associated with IT processes, people and systems. WBC drives the risk and governance frameworks, risk appetite, policies and standards from top down. WBC then uses the three lines of defence to report and escalate from the bottom up:

- the 1st line of risk defence is embedded in the business unit and forms part of the business unit management function. At this level the business unit manager is responsible for managing risk within the corporate risk management framework and risk appetite for the business unit.
- the 2nd line of risk defence is the group and divisional risk management business units that are tasked with expertise and governance of the risk management function within the corporate risk and governance framework. The risk management team also have accountability of approving delegation of authority and the risk exposure proposed by the business unit.
- the 3rd line of risk defence is the group assurance business unit. It provides independent oversight of adherence to the risk and governance frameworks across all business units and has a direct line of escalation to the Board.

4.2.3.2 WBC – Governance Framework

Figure 4.12 demonstrates the corporate governance structure at WBC.



Source: WBC 2013 Annual Report, p. 26

Figure 4.12 – WBC Corporate Governance Structure

In Figure 4.12 clearly shows that the non-executive leadership (the Board) and the executive leadership are kept separate. This is 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 sits as 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 as seen in Figure 4.12. Unlike CBA's risk committee that includes all of its Executive Board, the WBC risk management committee includes all the Executive Board members except for the CEO. The risk management committee sets and monitors the risk framework and risk thresholds on behalf of the bank. It also acts as the point of escalation and resolution for risks that fall outside of the risk framework or the thresholds set by the Board's risk committee. WBC has an additional committee that reports to the Board and that is 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.

4.2.3.3 WBC – Risk Position from the Analysis

The data presented in Table 4.9 was extracted from the data analysed carried out on the WBC's annual reports (WBC 2009, 2010a, 2011, 2012, 2013). The information gathered was used to establish the parameters that allowed the research to calculate the impact rating shown in Table 4.10 for each component of risk that was identified as needing to be managed as part of the bank's sourcing strategy. These impact ratings can be used in a future study as part of an objective questionnaire that can be used as part of a structured interview.

Table 4.9 – WBC Impact Rating Measurement

Component of Risk Management	Rating	Evidence
Governance and Risk Management	Very High	WBC's governance and risk management is untested except for their BCP component. The potential risk impact is very high until scenario or simulation models can demonstrate the governance and risk management framework provide sufficient protection.
Skills and Knowledge Management	Very High	18 major IT Projects
Companies fit and Alignment	Medium	A published vendor selection process exists and has been in use since 2009 but no results have been published. (Medium = Published and used for more than 3 years.)
Quality Management	Very High	Less than 3 years, started as a SIP program
Sovereign Risk / On-Going concern	Very High	8 offshore delivery centres in five different states
Offshore facilities (capacity for growth)	Very High	8 offshore delivery centres in five different states
Commercial	Very High	5 IT service providers (1 Infrastructure and 4 application)
Sustainability	Medium	Less than 50% of application services provided from an offshore delivery centre
Critical projects	Very High	18 major IT projects
Data Leakage and Confidentiality	Medium	Less than 50% of application services provided from an offshore delivery centre
Service Provider Mix	Very High	5 IT service providers (1 Infrastructure and 4 application)

Using the research approach outline in Section 3.2 to develop the WBC risk profile, Table 4.10 shows the results from the data analysis from WBC.

Table 4.10 – 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 4.13 shows the risks map based on the impact and probability results shown in Table 4.10.

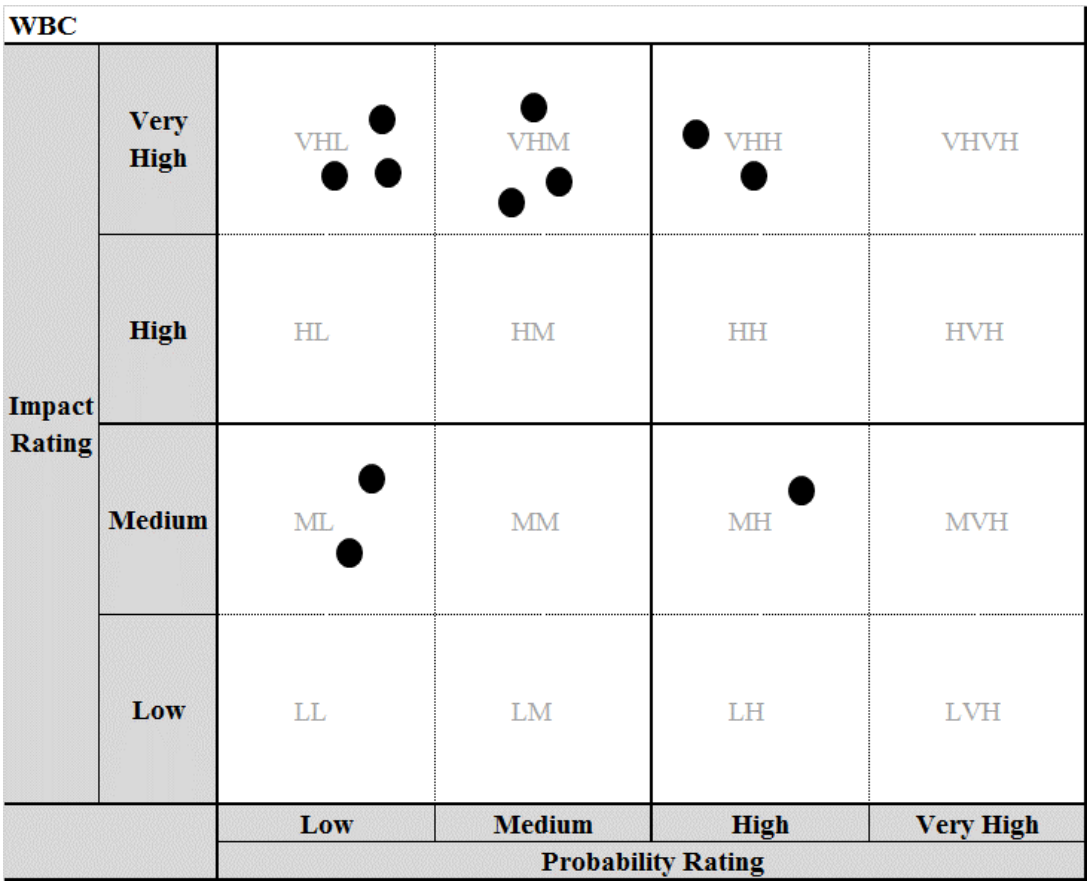


Figure 4.13 – WBC Risk Map

Each black dot on the map represents one risk category from the risks listed in the risk profile (Table 4.10). This analysis provides a simple picture of the risk spread.

The author has not associated mitigation activities to these risks as there is no need to over-complicate the picture by labelling each of the risk dots.

It can be seen in Figure 4.13 that the impact of the risks identified in Table 4.10 are predominately in the top left quadrants of the map with the next dominant quadrant being the top left. This tells us that the impact to the bank for the majority of the risks would be extremely high but the probability of risks being realised for the majority of the risks is fairly low. This indicates the bank needs to manage its risk profile very closely. WBC needs to apply a high level of focus at the senior management and executive level to ensure there is adequate attention and monitoring in order to control the risks. This could explain why WBC set up a technology committee reporting directly to the Board. This would give the right level of focus of any potential impacts the SIP initiatives and the changes in the IT sourcing strategy may have. Not articulated in the risk profile or the risk map is the details on any mitigation programs in place to address the risks.

4.2.4 Consolidated Findings of the Bank IT Sourcing Analysis

Table 4.11 sets the scene from an AFSI perspective and should be used as the baseline IT multi-sourcing model based on the sample of the two largest banks within APRA governance jurisdiction. In Chapter 5 there is a further exploration of how this trend analysis could be extended by using information from the other banks in the AFSI and the end state picture. There is also a discussion of the ramifications that the trends identified in this study could have on the AFSI and the Australian economy if any of the risks were to be realised. In the remainder of this section we examine the guidelines issued to the banks by APRA and BCBS on technology and IT sourcing risk management and governance. There is also a review of how technology and IT sourcing risks are governed at an industry level and if there are there any gaps in the industry level governance model.

4.2.4.1 Consolidated Industry Risk Position

From the data extracted, analysed and presented in sections 4.2.2 and 4.2.3 on the IT delivery models used by each bank this study has combined the options used by each bank and presented a consolidated view shown in Table 4.11.

Table 4.11 – Consolidated Bank IT Sourcing Analysis

Consolidation of the bank level IT Sourcing Results	Method of Delivery			
	Outsource	Outsource Offshore	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 consolidated information presented in Table 4.11 can be used in a future research project to develop the view of the IT delivery landscape at the AFSI level. For this current research project the data presented in Table 4.11 clearly demonstrates the AFSI has an extremely complex IT multi-sourcing model based on the sample. The challenge for APRA is to consider if the current prudential standards, risk and governance models afford sufficient protection to the economy from the risks associated with this level of complexity.

4.2.4.2 Projected Risk Profile Based on the Current Analysis

To complete the picture of the results based on the data extracted and analysed there is a need to look at the potential industry profile created by the banks' current IT sourcing activities. To assist in this analysis the following two tables and one figure were developed from the data presented on the two banks in the sample.

The next table, Table 4.12, is a consolidated view of the human resources and IT spend data for the two banks.

Table 4.12 – Consolidated IT Trend

Human Resource Data	2009	2010	CBA 2011	2012	2013
Total FTE Headcount	44,218	45,025	46,060	44,844	44,969
IT FTE Headcount					
IT Contractors	3,859	3,884	3,795	3,818	3,764
Total FTE	48,077	48,909	49,855	48,662	48,733
Human Resource Data	**2009**	**2010**	**WBC 2011**	**2012**	**2013**
Total FTE Headcount	37,032	38,962	37,806	35,675	35,597
IT FTE Headcount	8,530	11,174	11,600	10,058	10,163
IT Contractors					
Total FTE	45,562	50,136	49,406	45,733	45,760
IT Spend in millions AUD$	**2009**	**2010**	**CBA 2011**	**2012**	**2013**
Internal	$873	$1,029	$1,193	$1,159	$1,299
Outsourced Services	$689	$776	$932	$894	$977
Outsourced-Offshoring Services					
Total	$1,562	$1,805	$2,125	$2,053	$2,276
IT Spend in millions AUD$	**2009**	**2010**	**WBC 2011**	**2012**	**2013**
Internal	$1,429	$1,513	$1,456	$1,472	$1,506
Outsourced Services	$514	$526	$592	$620	$587
Outsourced-Offshoring Services	$249	$280	$254	$278	$350
Total	$2,192	$2,319	$2,302	$2,370	$2,443

Table 4.12 show a picture of two banks that report primarily the same information in two ways. This provides a slightly different picture of each bank.

CBA appears to have a high FTE headcount that is supplemented by a steady number of contractors in the IT space. CBA's IT expenditure appears to be increasing. The internal spend on IT services and the percentage spend on external IT services is roughly kept in the same percentage of total IT spend.

Then when there is an examination of WBC's IT headcount (in relation to overall headcount within the bank), the headcount increases for the first three years 2009 to 2011 then starts decreasing again from 2012 to 2013. WBC appears to spend more on internal IT services than CBA but spends approximately the same as CBA on external IT services. WBC does provide a better picture of where it spends its money on external IT services. The total spend on IT services between the two banks shows a dramatic difference in the amount spent in 2009 but over the five year period it appears the difference in the IT spend between the banks is narrowing.

This consolidated trend shows that whether a bank is using two or more delivery methods the overall impact on IT spend is not that great. So it could be construed the changes in IT delivery strategy to a multi-sourcing strategy does not deliver major cost savings. It may contribute to cost containment with the increase in transformation and modernisation activities in each of the banks.

In the next table and figure there is an analysis of the potential consolidated impact on the risk position from the evidence collected and presented on the two banks in this study. Table 4.13 shows the combined risk profile from the data obtained from the banks and analysed in this study.

Table 4.13 – Consolidated 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

Table 4.13 shows that if the worst case scenario is considered for each risk category, the impact rating shows a high number of very high impact risk categories. When this was then applied to the AFSI, and if a number of these risks were realised, they could have a major impact on the industry and therefore could impact the Australian economy. The combined data does not change the probability rating to a great extent which is good provided a '*domino effect*' does not occur with the risk categories.

Figure 4.14 shows the combined risk map from the data analysed and presented from each bank.

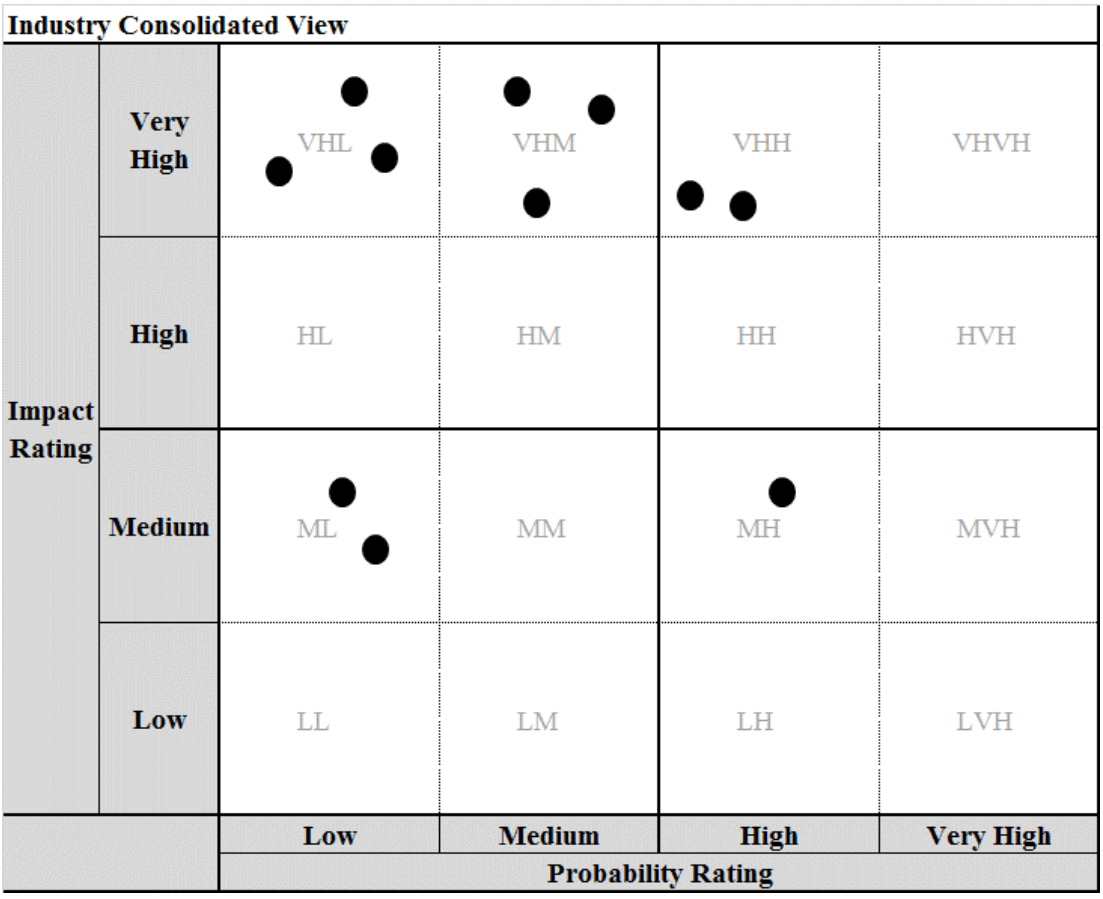


Figure 4.14 – Consolidated Risk Map

Each black dot on the map represents one risk category from the risks listed in the consolidated risk profile (Table 4.13). For the analysis in this study this provides a simple picture of the risk spread. There are no associated mitigation activities to these risks, so there is no need to over-complicate the picture by labelling and associating each of the risk dots with the relevant risk. The combined risk map paints a picture of the majority of risk categories located on the very high axis of the impact rating. On the probability axis the risks appear to be evenly spread in the first three quarters. Therefore the combined effect on the industry could be very high if the risks are not managed tightly at the bank level.

4.3 Patterns of Qualitative Data Analysis for Each Research Question

In Chapter 1 a conceptual model was presented in Figure 1.3. From this model three propositions were formulated to articulate the underlying assumptions of the conceptual model. Each of these propositions will now be addressed based on the analysis carried out on the data extracted in this study from the banks' web sites and from the regulatory governance organisation APRA.

P1. Each of the banks' business units select sourcing models based on their individual needs and they govern and manage their own operation risk.

From the risk management frameworks detailed for the banks it is clear the banks' business units do make decisions based on their individual needs. The constraints placed on them by the banks is the assessment, measurement and reporting of the risk associated with the decision.

P2. Each bank uses a single risk framework based on the APRA (2013a) guidelines for the governance and management of operational risk across all of the bank's business units.

From the analysis it is evident that the banks have adopted the risk framework proposed under Basel 11 and documented in the APRA prudential standard APS 115 published originally in 2007 and revised and issued in 2013. APS 115 outlines the guidelines for the risk management framework and advanced measurement approaches to operational risk (APRA 2013a).

P3. APRA's risk framework does not govern the cumulative industry operational risk associated with the individual banks' business units' selection of an IT sourcing model.

There was no evidence discovered during this study that demonstrated any consolidation of risk across the AFSI from an operational risk perspective. Each bank reports a consolidated position on operational risk that uses the same baseline measurement approach AMA. No evidence was identified from the study that showed any risk modelling at the industry level associated with technology or sourcing strategies associated with the banks activities.

The problem and propositions that arose in Chapter 1 and the research questions from chapter 2 are discussed in more detail in Chapter 5, the discussion chapter and summarised in Chapter 6, the conclusion and implications chapter.

4.4 Conclusion

In this chapter the author has reviewed the data available in the public domain for the banks, APRA, Basel committee and the IT service providers. The data shows consistency across both the banks and the regulators with regard to risk frameworks in use and their measurement of operational risk through the use of AMA. The Annual Reports from both banks raised some concerns with regard to inconsistencies in the way the information is presented in relation to their IT sourcing delivery models and the level of transparency provided.

The questions and inconsistencies in relation to the banks' and APRA's approach to the management of the risks associated with IT offshoring uncovered in the analysis of the data are discussed in more detail in the next chapter where there is a review and comparison of the analysis presented in this chapter and a presentation of alternative scenarios that can be construed from the data are analysed. To complement the data presented, there is more detail on the implications that of the lack of transparency of the IT sourcing delivery information and the implications this could have.

Each of the banks' modernisation programs includes multiple projects from critical projects such as replace the core banking platform to restructuring the internal governance and shared service organisations. The banks have published details of these projects and from the data included in the media releases and annual reports we can uncover projects that have been outsourced to external services providers. The modernisation programs are replacing the current systems and business processes. As part of building these new systems, the system documentation and training that forms part of the Service Delivery Life Cycle (SDLC) are handed over to the 'business as usual' groups to managed the systems going forward. Some programs are made up of pure IT projects e.g. replacing the service bus. Other programs are a mix of business process and IT project such as replacing the branch platform. Finally there are programs are made up of pure business process projects such as mortgage processing. Each project type carries its own set of skills and knowledge. If the bank does not

ensure this set is passed over to the current internal support organisation then it runs the risk of a knowledge gap when or if a problem occurs at a later date. Also the number of projects being executed at once has an impact on the risk rating as the interdependencies between the projects could have a domino effect if a problem occurs in one project.

Although the analysis of each bank in the sample has provided the data to develop a sourcing landscape, the data is inconsistent with the banks' sourcing strategies within the industry. For the purposes of this study there is not scope to provide confirmed empirical evidence without carrying out interviews with the decision makers from the banks. Again, each bank has implemented a risk framework, measurement methodology and governance model that aligns perfectly with the APRA requirements in (APRA 2013a). The analysis of the risk data from the banks and APRA raises the question: *does the operational risk measurement and capital adequacy model currently in use in the AFSI actually provide the level of transparency and accountability needed to manage IT multi-sourcing strategies that are being used to enable major modernisation and transformation programs that are taking place with the banks?*

Chapter 5 Discussion

This chapter provides the discussion on the findings from the analysis presented in the previous chapter. Figure 5.1 provides an overview of the discussion chapter.

5.1 Introduction

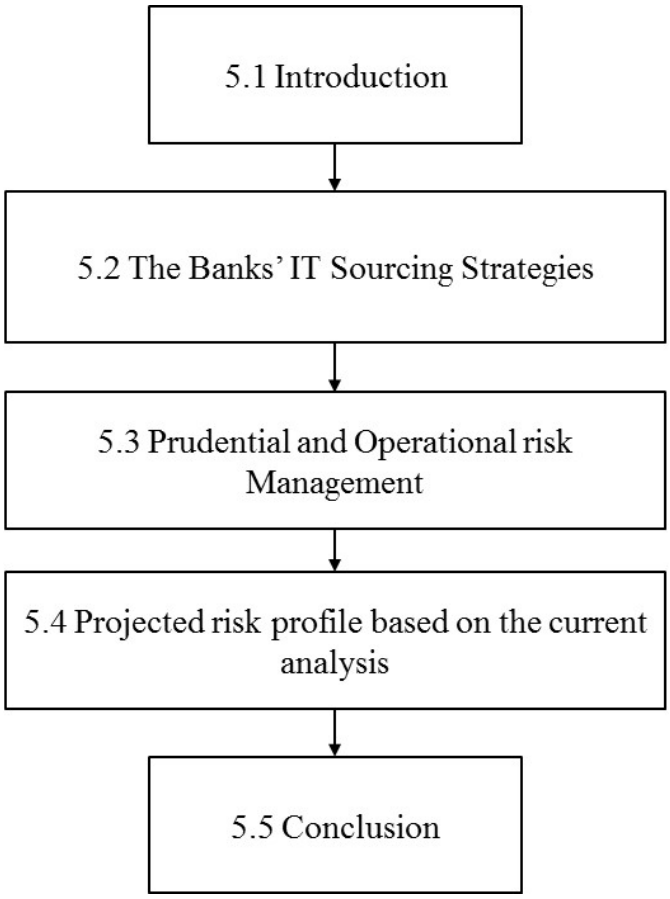


Figure 5.1 – Chapter 5 Structure

Section 5.1 is the introduction to the chapter and lays the foundation for the chapter and explains the structure of the chapter. Section 5.2 provides a discussion on each of the bank's IT sourcing strategies and the projected impact on the AFSI IT sourcing landscape based on the analysis of the data collected from the banks and regulatory bodies. Section 5.3 provides a discussion on the role of APRA from a prudential and operational perspective and evaluates if APRA provides enough economic protection from systemic risk. Section 5.4 discusses the impact on the AFSI risk profile and the industry if certain scenarios happen. Section 5.5 provides a summary for the chapter along with a link to the final chapter, the conclusions and implications chapter of the dissertation.

5.2 The Banks' IT Sourcing Strategies

The findings on CBA and WBC from the analysis of data presented in Chapter 4 are now reviewed to discover the implications to the stability of the banks and the AFSI.

CBA has a consistent risk management and governance model that spans the company from the business unit level up 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 2013a) and the implemented model as documented in the Annual Report (CBA 2009).

5.2.1 CBA IT Sourcing Strategy

The analysis of the CBA data highlighted a number of major concerns that are discussed in this section.

5.2.1.1 Technology Committee

From the analyses it appears that unlike WBC, CBA does not have a technology committee that reports to the bank's Board. The CBA has been and is going through a major IT transformation and modernisation programs (Bennett 2012; CBA 2011a). It makes sense that with the potential risks associated with these transformational and modernisation initiatives the Board level would want direct visibility of the projects and programs being implemented. It could be argued that part of the current risk management framework should provide the Board with sufficient visibility. Within the data reviewed it appears the technology or IT change programs are wrapped into the operational risk reports. It appears there is no direct line of sight from the Board level of these major changes and therefore risks associated with the changes.

5.2.1.2 CBA States "they do not offshore bank jobs"

Claims have been made by the CEO of the CBA that they do not offshore Australian bank jobs. A review of the bank's media releases both from the current and previous leadership (CEO & CIO) clearly state that CBA do not offshore bank jobs (Newman 2013; Tait 2012). Although the leadership of CBA states that CBA does not offshore bank jobs, from the evidence collected and presented in the analysis of data in Chapter 4, it is clear that CBA certainly does have the capability to use its current IT service providers' offshore capabilities to deliver IT services to CBA without impacting current bank jobs. A future study could aim to qualify if CBA has any services delivered from any offshore locations.

5.2.1.3 IT budget and expenditure

The IT budgets and expenditure extracted from the annual reports and presented in the analysis of data chapter 4 do not follow standard patterns that would be expected in a large corporation. Searches for information on why the IT expenditure data fluctuated to the extent that it did failed to uncover the reasons for the variations. The expenditure on both internal IT services delivery and IT services supplied from external service providers showed a year on year increase in expenditure between 2009 and 2011. In 2012 both internal and external lines of IT service delivery decreased then in 2013 increased again. The unusual pattern in 2011 and 2012 could possibly be investigated in a future project.

5.2.1.4 Why did material projects reporting change?

Up until and including the 2011 annual report, CBA published a list of long term and material technology contracts that it had signed similar to those of WBC. Since the 2012 annual report, no statements on material or long term CBA contracts with external IT services providers are provided. Searches to identify a reason why CBA stopped producing this information found no results. This research raises the question 'why did CBA stop reporting on material projects and engagements?' which could be addressed in future studies.

5.2.2 WBC IT Sourcing Strategy

The findings presented in the analysis of data Chapter 4 demonstrate that WBC has a complex IT sourcing model that has continually evolved due to changes in the market and technology (WBC 2010b). The drivers articulated by the CEO of WBC seem to align with the decision theories discussed in the literature review. During an interview at a visit to one of Westpac's operations centres in India in February 2013, CEO Mrs Kelly defended the practice of outsourcing and offshore-outsourcing by saying: "*It had allowed the bank to work with "world-class" companies such as IBM and given it access to highly skilled workers. The strategy is not about cost arbitrage, the strategy is about skill enhancement*" (Yeates 2013).

WBC has a robust risk management and governance model that spans the company from business unit level 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 2013a) and the implemented model as documented in the Annual Report (WBC 2009).

On the surface it appears from a bank and regulatory perspective that there is a sound foundation to claim WBC manages its operational risk within the regulator's guidelines. One difference uncovered in the analysis was that while WBC has a clear definition for technology risk, no definition for technology risk could be found in the APRA standards. Hence the main governance body APRA does not appear to provide clear guidelines on technology risk and in particular the IT risks associated with IT multi-sourcing.

During the analysis of the WBC data a few questions were raised that should be addressed. These questions are addressed in the remainder of this section.

5.2.2.1 WBC Risk Committee Structure

Why does the WBC risk committee exclude the CEO? The analysis of the CBA data showed that it includes the CEO on the risk committee. The data analysis did not provide any insight into the rationale behind this decision. The answer to 'why is the CEO of WBC excluded from the risk committee?' could be investigated in a future study.

5.2.2.2 WBC Definition of FTE

WBC includes contractors in its FTE headcount. This is not the normal practice as FTEs form part of the core budget and usually only includes permanent staff. The reason for separating the two types of employees is because the permanent staff budget takes into account corporate overheads such as superannuation, long service leave, annual leave and sick leave. Contractor budgets do not usually include these overheads as the contractor is normally paid a 'fully loaded' hourly or daily rate. 'Why does WBC include contractors in the FTE headcount in their annual reports?'

5.2.2.3 WBC Technology Committee

WBC has set up a technology committee that reports directly to the Board. The evidence shown in (WBC 2010b) indicates the technology committee setup to provide the Board with direct visibility of the SIP programs thus assist with the governance and management of the risk associated with the SIP initiatives. If WBC views the risk associated with the changes introduced by the SIPs as needing visibility at Board level, then why does WBC not report the technology risk to APRA separately from its operational risk report to APRA so the technology risk and mitigation activities can be seen?

5.3 Prudential and Operational Risk Governance

APRA has provided a risk framework, guidelines and method of assessing risk (APRA 2013a) and from the analysis of the banks' information both banks comply with the APRA risk requirements. APRA developed the prudential standards used in the AFSI based on the Basel Committee accord, white papers and guidelines (Basel Committee on Banking Supervision 2004, 2005, 2011a, 2011b). This research has found no evidence that the banks have diverged or disagreed with either APRA or Basel Committees directives.

A gap may have been identified in the treatment of risk associated with IT transformation, modernisation and IT sourcing and whether the current operational risk framework, guidelines and methods are sufficient to provide enough proactive protection across the AFSI.

APRA has published two prudential standards that in combination attempt to address the IT sourcing strategy undertaken by the banks (APRA 2005, 2006). One could argue that these standards provide sufficient protection because they address outsourcing and business continuity planning. What the APS 231 and APS 232 standards appear to have missed is the variance in levels of risk that would arise if a bank outsources IT, offshores IT or offshore-outsources IT. Also they do not address the banks' use of multi-sourcing for IT services. A combination of delivery models across the different functions of IT services provides another level of complexity.

If this complexity is considered at an industry level with multiple banks adopting different mixes of delivery models to supply IT services to their customer, a number of questions are raised. Are the current prudential standards sufficient to ensure the industry level risk is being addressed without explicit industry level governance? Is operational risk sufficient to handle technology risk, especially when the banks are going through major technology modernisation? Should there be a risk category for IT sourcing risk?

5.4 Projected Industry Risk Profile

To complete the discussion of the results from the data analysed in Chapter 4 there needs to be an examination of the potential industry risk profile created from the banks' risk profile which is based on their current IT sourcing strategies. The consolidated trend (Table 4.10) shows that whether a bank is using two or more delivery methods the overall impact on IT expenditure does not appear to be that substantial. So it appears that the banks' move to IT multi-sourcing has failed to deliver major cost savings, but does affect the risk profile for both the individual banks as well as the industry. It could be argued that the banks' IT multi-sourcing strategy contributes to cost containment of the costs associated the transformation and modernisation initiatives both banks are engaged in.

In Table 4.11 a consolidated risk profile was presented. Taking into consideration the top three risks at an industry level, '*skills and knowledge management*' requires the banks to retain sufficient resources and experienced staff to keep the systems operating if they were brought back in-house. '*sustainability*' raises the question: at what point would a bank relinquish so much control that they would no longer have the skills or staff to repatriate the IT functions? Finally, '*critical projects*' refers to the situation where the banks' new transformed and modernised systems do not have any IT staff in the banks able to understand and support the new systems. Interestingly enough, the owners of these three risks are the banks' IT

delivery business units. This places the risk squarely in the technology space which is not measured or reported at an industry level.

5.5 Conclusions

IT services are dependent on systems, processes and people. In many cases the risk capital provision associated with the delivery of IT services may not align with the likely impact on the bank's reputation if IT services fail. IT systems may not align to the criticality of the business function and therefore may not form part of the risk capital provision. The bank's business and IT services processes may be recognised as not having any monetary value within the risk capital calculation. With human resources, calculating the dollar value based on the functions they perform does not always align with their remuneration package. Salary levels do not always equate to the criticality of the function they perform.

Consider an example of a potential catastrophic scenario. The failure of one IT system, its processes or personnel could have a negative impact on the AFSI and Australian economy. As an example the IT payments system fails at one of the banks and the overnight processing of payments cannot be performed. Similar incidents to this have occurred in the past (Budd 2011; Foo 2011). The bank cannot recover the system and complete the payments run in time to process the payments before start of business. None of the other banks are able to assist by performing 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 government, business and individuals defaulting on loan payments and could result in total financial and economic collapse similar to that felt by the great financial crash in the USA in 1929 or the GFC in 2007-2008.

Although both banks in the sample adhere to the standards and guidelines published by APRA, the internal IT delivery models and implementation of the risk framework differ with regard to the delivery of IT services. These differences do demonstrate that IT service delivery should be given more focus and guidance by APRA. There is no evidence of how a critical situation could be addressed if a major IT system or process failed. The calculation of risk provision using AMA is based on market and company historical data (APRA 2013a). Is there sufficient historical data to provide realistic risk provision associated with current IT multi-sourcing practices in the AFSI? Is AMA the correct method to use in calculating such risk?

In the final chapter there is an examination of the results produced in the analysis of data (Chapter 4) the research problem and propositions introduced in chapter 1 are addressed, as are the research questions introduced in Chapter 2 of this thesis. The author also outlines future planned research projects that will use the data and findings in this Master's research project to develop a more in-depth project that will involve engaging with the banks and the regulator to address the gaps and questions uncovered as part of this research project.

Chapter 6 Conclusions and Implications

This final chapter provides a summary of the Masters' research project and its findings. It presents the conclusions derived from the research along with the implication and suggestions for future research. Figure 6.1 provides an overview of this chapter.

6.1 Introduction

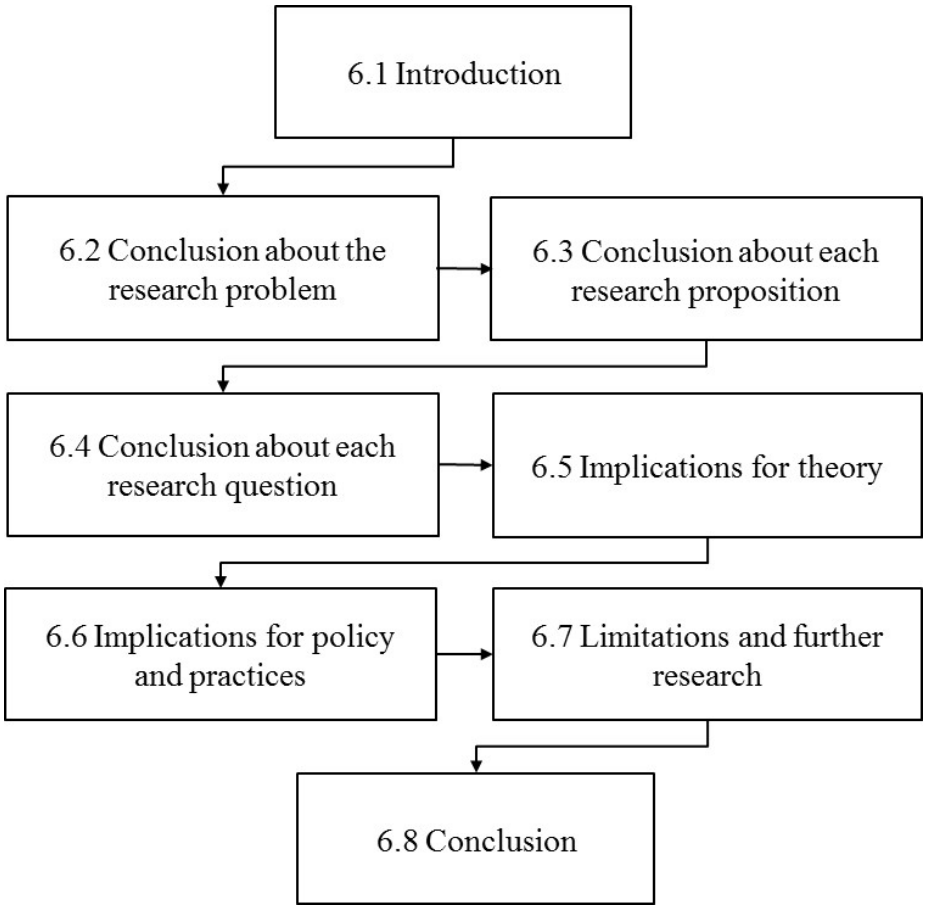


Figure 6.1 – Chapter 6 Structure

Section 6.1 is the introduction to the chapter that lays the foundations for the chapter and describes the structure of the chapter. Sections 6.2, 6.3 and 6.4 provide conclusions to the problem and propositions that were introduced in Chapter 1 and the research questions from Chapter 2. Sections 6.5 and 6.6 outline the contribution of the study to the academic theories, policies and practices discussed in chapter 2. Next section 6.7 outlines the limitations of the research and proposes further research that could be carried out using the data from this study as its foundation. Finally section 6.8 provides a summary for this chapter along with a summary and conclusion for the dissertation.

6.2 Conclusions about the Research Problem

The research problem articulated in Chapter 1 states: '*Concerns have been raised about the adequacy of APRA's guidelines to manage the banks' multi-sourcing IT service delivery strategies (Bennet 2012; Durie & Gluyas 2009; Flinders 2014). Furthermore, given the multi-sourcing approach to IT service delivery by the banks*

would there be a negative impact on the banking sector or even on the economic risk profile of the Australian economy if a catastrophic event were to occur?'

The evidence discovered from the data analysis carried out on the public domain documents from CBA and WBC suggests the banks have moved to a higher level of IT sourcing delivery complexity than APRA (2005) and APRA (2006) were designed to govern. The risk framework outlined in APRA (2013a) is adhered to by both banks but it is unclear if the complexity of the multi-sourcing strategies implemented by both banks to deliver IT service is adequately covered.

6.3 Conclusions about the Research Propositions

The research propositions as outlined in Chapter 1 are:

P1. Each of the banks' business units select sourcing models based on their individual needs and they govern and manage their own operation risk.

The risk management frameworks for the two banks detailed in Chapter 4 demonstrate that the banks' business units make decisions based on their individual needs. The main constraint placed on the business units by the bank's Board is the risk threshold allowed. This limit controls how much risk each business unit is allowed to provision for without impacting the overall threshold of the bank.

P2. Each bank uses a single risk framework based on the APRA (2013a) guidelines for the governance and management of operational risk across all of the bank's business units.

From the analysis it is evident that each bank has adopted and implemented the risk framework outlined in the APRA prudential standard APS 115 published originally in 2007 and revised and issued in 2013 (APRA 2013a).

P3. APRA's risk framework does not govern the cumulative industry operational risk associated with the individual banks' business units' selection of an IT sourcing model.

There was no evidence that demonstrated any consideration of the consolidation of risk by APRA across the AFSI. Each bank reports a consolidated position on operational risk that uses the same baseline measurement approach AMA. There was no evidence of risks associated with technology changes or IT multi-sourcing strategies associated with the banks' activities.

6.4 Conclusions about the Research Questions

The research questions developed and presented in Chapter 2 are:

RQ1. Do the banks employ complex multi-sourcing solutions driven by business unit demands to deliver their IT services?

From the analysis of the two banks, the evidence shows that both banks have not only a complex multi-sourcing environment to deliver IT services, they also have a multi-vendor environment. CBA uses outsourcing and in-house IT delivery models and at least four external IT service providers to deliver IT outsourcing solutions in the infrastructure and application delivery environment. WBC uses outsourcing, offshore-outsourcing and in-house IT delivery models and at least four external IT service providers to deliver IT offshore-outsourcing solutions in the application delivery environment and one IT outsourcer to deliver IT infrastructure services. This 'multi-vendor-multi-sourcing' provides another level of complexity that was not considered in this research project and can be factored into the future research.

The business units of each bank are the customers of the internal IT service provider. The business units provide the IT funding so they are one of the main drivers behind the IT business units need to lower costs and increase quality to meet the business units' demands. The modernisation programs introduced by both CBA and WBC have a strong focus on improving the customer experience. Examples of these are the branch modernisation, online banking and mobile banking. The demand for change comes from customer feedback via the customer facing business units such as the retail banking business and the institutional banking business unit.

RQ2. What are the risk and governance model/s used by the banks to manage risks associated with their IT services multi-sourcing strategy?

Both banks use very similar risk and governance models that are based on the recommendations proposed by APRA. These models have a good fit when managing prudential risk and even in the general operational environment. The challenge is that neither bank appears to have factored in any risk associated with the 'multi-vendor-multi-sourcing' IT delivery model they have used. Only WBC has separated the technology risk associated with the introduction of the SIP initiatives, which from WBC's risk management and corporate governance perspective is an excellent move. However, the prudential regulations associated with outsourcing and operational risk management (APRA 2005, 2006, 2013a) monitor one delivery method and measure the risk associated with technology changes. APS 231, 232 and 115 standards do not monitor and measure the risk impact of the bank using a multi-sourcing delivering to deliver the IT change programs.

RQ3. Is the AFSI IT operational risk exposure adequately covered by the current APRA risk framework and prudential standards?

No evidence was found during the analysis of the data from APRA that any industry level consolidated reports on operational risk are published. Actually, in the prudential standards it is made clear the calculation of capital risk, management of risk thresholds and the process of managing risk is within the bank's total control. APRA will not intervene provided the banks stay within the published risk guidelines. It appears from the key findings of the data analysis that APRA does not factor in any '*domino effect*' nor does it account for the risk associated with how IT services are sourced other than the outsourcing prudential standard which seems to be focused on customer data protection and BCM.

6.5 Implications for Theory

This research draws on the theories discussed in Chapter 2 as the foundations for the risk analysis performed on the data gathered from the banks. There appears to an absence of academic literature that applies the use of decision theories to explain the use of multi-sourcing strategies for IT Services within the financial services industry.

The literature reviewed in Chapter 2 suggests that we can consider decision theories for outsourcing and offshore-outsourcing based on the two phases of outsourcing: the initial decision to outsource, and the subsequent decision to offshore-outsource. Transaction Cost Economics (TCE) (Coase 1998) and agency theory (Eisenhardt 1989) help us to understand the banks' decision to outsource. TCE focuses on reducing costs and agency theory explains shifting technology innovation risk to the service provider. One of the outcomes explained by agency theory is the ability to

shift risk from the principal to the agent and therefore mitigate the risk associated with delivering the service. In APRA (2006) it clear that from an APRA perspective outsourcing increases risk and therefore requires mitigation to be put in place. So the ability of an Australian bank to use 'shifting risk to an external services provider' as a reason to outsource would be rejected by APRA under the current prudential standards. In the second phase, when the bank decides to offshore-outsource, agency theory is still relevant but TCE provides a more compelling theoretical explanation as the evidence shows that offshore-outsourcing provides more cost savings due the lower resource costs. The ability for the principal to shift the risk to the agent is reduced further due to the agent being outside the local jurisdiction and therefore not under the same regulatory constraints as a local service provider.

The results shown in Table 4.1 indicate that a complex IT delivery model exists within each bank as a result of decisions made over a period of time. These complex IT delivery models have an associated complex risk matrix. This study demonstrated this complexity and highlighted the cumulative risk matrix at the industry level.

This research has contributed to our understanding of the cause and effect of individual bank's decision making strategies on the Australian finance industry. The analysis highlights how the current risk management models used within the AFSI could be enhanced based on comparative research of the finance industry in another region (Alexander 2006).

6.6 Implications for Policy and Practice

APRA's prudential standard on risk and provision of capital adequacy using AMA (APRA 2013a) seems to provide a sound risk framework to manage operational risk in a consistent and stable environment. But from the findings of this study neither of the banks could be considered to be in a consistent and stable environment especially from a technology perspective. It could be suggested that the current prudential standard on operation risk management is sufficient to govern a RTB environment. But the current prudential regulations on operational risk are not sufficient to manage operational risk when the bank is going through major strategic CTB transformation and modernisation programs. The current prudential standards use capital adequacy to mitigate the risk e.g. enough financial reserves to address the risk if it is realised. In the technology environment, financial reserves may not be the ideal way to mitigate risk. The impact of failure is immediate and time is the enemy as consumer confidence is undermined the longer a problem exists. Therefore it is suggested that a proactive risk management framework is needed rather than the reactive risk framework currently used by APRA in the prudential standards.

APRA outlined the standards that the banks need to adhere to in order to meet the prudential standards ASP 231 and ASP 232. It has been clearly demonstrated that the banks meet these but the question still remains, are the prudential standards sufficient to meet the sophistication and complexity of the industry they were written to protect? The Basel 11 accord outlines the risk framework that financial institutions need to meet and APRA has adopted this framework and is enforcing it within the AFSI. Again the question remains, the risk framework was built to manage prudential risk: is the framework sufficient to manage operational risks associated with multi-sourcing of IT services practiced in the AFSI?

The mitigation strategies outlined in Willcocks, Lacity and Kern (1999) could be used by APRA as a foundation to review the risk framework outlined in APS 115 (APRA 2013a) to extend the prudential standard to include proactive mitigation strategies that the banks would need to implement. This proactive mitigation could be

based on specific IT services rather than as it is currently 'lumped' under a generic umbrella of IT services. Willcocks et al. demonstrate this in their research case study into managing risks associated with IS outsourcing of the Logistics Information Systems Agency (LISA) which is part of the UK defence agency to EDS. APRA could ask each bank to identify the core services and non-core services the bank views as imperative to the stability of the services provided to its customers. Next APRA would require each bank to identify which IT systems underpin the delivery of each service. Finally a complexity matrix could be drawn up to show the risk profile for each service if it was delivered either in-house, outsourced, offshore-outsourced, offshored or a combination of these delivery models. This complexity matrix could then be used to establish a risk governance approach for each service type. This approach would also enable APRA to roll the risk profiles up to an industry level to show the potential industry and economic risk exposure.

6.6.1 Recommendation to APRA

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 how complex the mix of IT service delivery models is 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.

6.7 Limitations and Further Research

The limitation is recognised that the analysis of the banks and governing bodies relies 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.

In a future research project, the author plans to use the data and findings from this study to carry out research that will extend the sample to include the four major Australian banks (WBC, CBA, ANZ and NAB). The secondary information gathered during the Masters research project will be drawn upon, and an extension applied to the sample period to include subsequent years from 2013 to the completion of the future project. This will provide an even more accurate picture of the banking industry level risk profile. This project will review the IT sourcing models used by the four banks to deliver their IT transformation and modernisation programs (CTB). This will demonstrate the complexity within the banks IT multi-sourcing models and the difference between each bank's models.

6.7.1 Limitation in Risk Profile Developed for this Study

The influence of cultural alignment is a factor in the success of the commercial relationship between an external service provider and customer. The question for this study is: is it a critical success factor? This weighting factor of the different risk components could not be measured in this study as it would require an interview with the decision makers to ascertain the weighting factor. So for this study all the risk components carry the same weighting e.g. 1 which does not differentiate between the risk components. The cultural alignment component is influenced by factors such as the maturity of the bank's commercial business unit, the maturity of their vendor selections process, and the use of IT service frameworks e.g. CMMi, COBIT, and ITIL. Although the banks have published vendor selection processes as directed by APRA, without investigation via interview the maturity cannot be derived. Also each bank uses industry standard IT service frameworks but again without talking with the people in the banks it is not possible to ascertain the maturity level of the bank within the framework/s they use. The external service providers all claim that they have achieved the highest level for each of the IT services framework/s they use so there is a potential for misalignment as IT is not viewed as 'core business' for the banks.

The use of the term sustainability in the context of this study has two lens. Firstly the likelihood of the service provider remaining in business long term. Except for IBM and CSC most of the current IT service providers have been in the industry for less than 15 years. Mismanagement and / or economic reasons can result in a service provider going into liquidation. An example of this was Satyam, a service provider based in India as a result of mismanagement went into liquidation. Some Satyam customers had major impacts on their ability to maintain their services while other service providers analysed the Satyam contract portfolio to identify the more lucrative contracts to take over.

The second lens looks at the complexity of the systems and commercial framework it uses and considers if it will allow the service provider to maintain a reasonable margin. The norm within a commercial framework is the narrower the margin the tighter the commercial control used to contain the scope and ensure all services are fully cost-recovered by the service provider. To consider service providers and sustainability in depth would result require another study as it would take the conversation in a completely different direction. Sustainability is used as a risk component that has influence on a bank's potential risk exposure.

6.7.2 Future Research

The future project will show how the Australian Prudential Regulatory Authority (APRA), the regulatory for the banking industry, provides risk guidelines and governance to the banks. The future research project will show the cumulative banking industry risks based on the risk profile associated with each banks IT multi-sourcing strategies. Finally an alternative risk management framework will be developed that will address the gaps in the current risk management framework based on the Basel accord.

This will extend the sample of the study and also the depth of the information collected so that the researcher can develop a new risk model and framework that could be used by the banks to manage multi-sourcing risk in the technology areas. The impact and probability ratings used in this study could not be verified by practice as this would have required contacting the risk component owners within each bank. In the proposed future research project the impact and probability ratings derived as part of this research project will be verified with the risk component owners with each

bank. Also APRA would be able to use the same model and framework to provide an AFSI level risk position.

Information gathered from this study could also form the foundation for a review of the prudential regulator in other jurisdictions and within banks of varied sizes. Also, if further research was carried out into other prudential jurisdictions and similar findings were uncovered, an international study into the impact on the domestic IT skills and capabilities retention and risk could be carried out.

There was not scope within this study to examine 'management fashion theory' but the application of this theory raises a number of issues could be addressed in a future study within this area. For example: d*o the same consulting companies develop the sourcing strategy for all of the banks? And did the decision-makers in each bank arrive at the same solutions in their previous organisation?*

6.8 Conclusion

The results of the study show a complex IT delivery model exists within each bank. This study has shown that each IT sourcing model has an associated complex risk matrix that requires management and governance.

Today each bank has its own business continuity plan which examines differing disaster scenarios on an annual basis. No evidence was found that showed APRA has a similar framework to the banks' BCP test that they carry out to test disaster scenarios at the industry level. If a comprehensive risk framework was developed, then like the prudential risk system it would need an allocation of funds to pay for remediation. But the framework would also need to have a proactive element similar to the business continuity plans where the scenarios are tested on a regular basis at the industry level.

This research has contributed to our understanding of the cause and effect of each bank's decision making strategies in terms of delivery of IT services on the Australian finance industry. Analysis highlights how the current risk management models used within the AFSI could be enhanced based on comparative research of the finance industry in other major developed countries that are part of the BCBS (Basel Committee on Banking Supervision 2004).

In conclusion, the aim of this study has been achieved: the analysis results demonstrated the complexity and risk of the current IT delivery environment within each of the banks. A risk assessment for each bank has been completed and a consolidated industry level view of the risks developed. This research will form a solid foundation for future research into the prudential regulatory risk management and governance of the banking industry within Australia. The study has contributed to filling some of the gaps in research around the critically important issue of risk governance and management. This study has shown the impact of banks' IT sourcing decision making on the risk profile of their bank and also the impact on the Australian economic stability. The results from this research show the current prudential risk governance framework introduced by APRA to the AFSI may not be sufficient to mitigate risks associated with the mix of IT sourcing models used by the banks.

Bibliography

Evans, D, Gruba, P & Zobel, J 2011, *How to Write a Better Thesis*, Third edition, Melbourne University Press, Australia.

Perry, C 2013, *'Efficient and effective research: a toolkit for research students and developing researchers'*, AIB Publications, Adelaide SA, Australia.

Appendix 1 – Cross Reference to Risk Component

APRA Categories (Category 2)	APRA Activity examples	Risk Component Alignment with APRA Category and Activity Example
Unauthorised activity	Transactions not reported (intentional) Transaction type (unauthorised) Mismarking of position (intentional)	Governance and Risk Management, Skills and Knowledge Management, Companies fit and Alignment, Quality Management Data Leakage and Confidentiality
Theft and fraud	Fraud/credit fraud/worthless deposits Theft / extortion / embezzlement / robbery Misappropriation of assets Malicious destruction of assets Forgery Cheque kiting Smuggling Account take-over/impersonation, etc Tax non-compliance/evasion	Governance and Risk Management, Companies fit and Alignment, Commercial Data Leakage and Confidentiality and Service Provider Mix
Theft and fraud	(Intentional) Bribes / kickbacks Insider trading (not on ADI's account)	Governance and Risk Management, Companies fit and Alignment, Quality Management, Sovereign Risk / On-Going concern, Commercial and Critical projects
Theft and fraud	Theft/robbery Forgery Cheque kiting	Governance and Risk Management, Sovereign Risk / On-Going concern Commercial, Data Leakage and Confidentiality
Systems security	Hacking damage Theft of information (with monetary loss)	Governance and Risk Management, Skills and Knowledge Management, Companies fit and Alignment, Quality Management, Sovereign Risk / On-Going concern, Offshore facilities (capacity for growth), Commercial, Sustainability, Critical projects, Data Leakage and Confidentiality and Service Provider Mix

APRA Categories (Category 2)	**APRA Activity examples**	**Risk Component Alignment with APRA Category and Activity Example**
Employee relations	Compensation, benefit, termination issues Organised labour activity	Governance and Risk Management Skills and Knowledge Management Companies fit and Alignment Quality Management Offshore facilities (capacity for growth) Commercial Sustainability Critical projects Data Leakage and Confidentiality Service Provider Mix
Safe environment	General liability (slip and fall, etc) Employee health and safety rules events Workers' compensation	Governance and Risk Management Companies fit and Alignment Quality Management Offshore facilities (capacity for growth)
Diversity and discrimination	All discrimination types	Governance and Risk Management Skills and Knowledge Management Companies fit and Alignment Quality Management Sovereign Risk / On-Going concern Offshore facilities (capacity for growth) Commercial Sustainability Critical projects Data Leakage and Confidentiality Service Provider Mix
Suitability, disclosure and fiduciary	Fiduciary breaches/guideline violations Suitability/disclosure issues (e. g. know your client requirements) Retail customer disclosure violations Breach of privacy Aggressive sales Account churning Misuse of confidential information Lender liability	Governance and Risk Management Skills and Knowledge Management Companies fit and Alignment Quality Management Sovereign Risk / On-Going concern Offshore facilities (capacity for growth) Commercial Sustainability Critical projects Data Leakage and Confidentiality Service Provider Mix

APRA Categories (Category 2)	**APRA Activity examples**	**Risk Component Alignment with APRA Category and Activity Example**
Improper business or market practices	Antitrust Improper trade/market practices Market manipulation Insider trading (on the ADI's account) Unlicensed activity Money laundering	Governance and Risk Management Skills and Knowledge Management Companies fit and Alignment Quality Management Sovereign Risk / On-Going concern Offshore facilities (capacity for growth) Commercial Sustainability Critical projects Data Leakage and Confidentiality Service Provider Mix
Product flaws	Product defects (unauthorised, etc.) Model errors	Governance and Risk Management Skills and Knowledge Management Companies fit and Alignment Quality Management Sovereign Risk / On-Going concern Offshore facilities (capacity for growth) Commercial Sustainability Critical projects
Selection, sponsorship and exposure	Failure to investigate client per guidelines Exceeding client exposure limits	Governance and Risk Management
Advisory activities	Disputes over performance of advisory activities	Governance and Risk Management Skills and Knowledge Management Companies fit and Alignment Quality Management Sovereign Risk / On-Going concern Offshore facilities (capacity for growth) Commercial Sustainability Critical projects Data Leakage and Confidentiality Service Provider Mix

APRA Categories (Category 2)	**APRA Activity examples**	**Risk Component Alignment with APRA Category and Activity Example**
Disasters and other events	Natural disaster losses Human losses from external sources (e.g. terrorism or vandalism)	Governance and Risk Management Skills and Knowledge Management Companies fit and Alignment Quality Management Sovereign Risk / On-Going concern Offshore facilities (capacity for growth) Commercial Sustainability Critical projects Data Leakage and Confidentiality Service Provider Mix
Systems	Hardware Software Telecommunications Utility outage/disruptions	Governance and Risk Management Skills and Knowledge Management Companies fit and Alignment Quality Management Sovereign Risk / On-Going concern Offshore facilities (capacity for growth) Commercial Sustainability Critical projects Data Leakage and Confidentiality Service Provider Mix
Transaction capture, execution and maintenance	Miscommunication Data entry, maintenance or loading error Missed deadline or responsibility Model/system mis-operation Delivery failure Collateral management failure	Governance and Risk Management Data Leakage and Confidentiality Governance and Risk Management Companies fit and Alignment Critical projects Service Provider
	Reference data maintenance	Governance and Risk Management Skills and Knowledge Management Companies fit and Alignment Quality Management Sovereign Risk / On-Going concern Offshore facilities (capacity for growth) Commercial Sustainability Critical projects Data Leakage and Confidentiality Service Provider Mix

APRA Categories (Category 2)	**APRA Activity examples**	**Risk Component Alignment with APRA Category and Activity Example**
Monitoring and reporting	Failed mandatory reporting obligation Inaccurate external report (loss incurred)	Governance and Risk Management Skills and Knowledge Management Companies fit and Alignment Quality Management Sovereign Risk / On-Going concern Offshore facilities (capacity for growth) Commercial Sustainability Critical projects Data Leakage and Confidentiality Service Provider Mix
Customer intake and documentation	Client permissions/disclaimers missing Legal documents missing/incomplete	Governance and Risk Management Commercial Data Leakage and Confidentiality
Customer/client account management	Unapproved access given to accounts Incorrect client records (loss incurred) Negligent loss or damage of client assets	Governance and Risk Management Skills and Knowledge Management Companies fit and Alignment Quality Management Sovereign Risk / On-Going concern Offshore facilities (capacity for growth) Commercial Critical projects Data Leakage and Confidentiality
Trade counterparties	Non-client counterparty mis-performance Miscellaneous non-client counterparty disputes	Governance and Risk Management
Vendors and suppliers	Outsourcing Vendor disputes	Governance and Risk Management Skills and Knowledge Management Companies fit and Alignment Quality Management Sovereign Risk / On-Going concern Offshore facilities (capacity for growth) Commercial Sustainability Critical projects Data Leakage and Confidentiality Service Provider Mix

References

Abrahamson, E 1991, 'Managerial Fads and Fashions: The Diffusion and Refection of Innovations', *Academy of Management Review*, vol. 16, no. 3, pp. 586-612.

Abrahamson, E 2011, 'The Iron Cage: Ugly, Uncool, and Unfashionable', *Organization Studies*, vol. 32, no. 5, pp. 615-29.

Agrawal, NM, Pandit, R & Menon, D 2012, 'Strategy to usher in the next phase of growth in the Indian IT industry', *IIMB Management Review*, vol. 24, no. 3, pp. 164-79.

Alavi, M & Leidner, DE 2001, 'Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues', *MIS Quarterly*, vol. 25, no. 1, pp. 107-36.

Alexander, K 2006, 'Corporate governance and banks: The role of regulation in reducing the principal-agent problem', *Journal of Banking Regulation*, vol. 7, no. 1/2, pp. 17-40.

APRA 2005, *Prudential Standard APS-232*, Business Continuity Management, APRA, Australia, viewed 06/03/2013, <http://www.apra.gov.au/adi/PrudentialFramework/Pages/prudential-standards-and-guidance-notes-for-adis.aspx>.

APRA 2006, *Prudential Standard APS-231*, Outsourcing, APRA, Australia, viewed 06/03/2013, <http://www.apra.gov.au/adi/PrudentialFramework/Pages/prudential-standards-and-guidance-notes-for-adis.aspx>.

APRA, *APRA Brochure*, 2010, APRA, Australia, <http://www.apra.gov.au/AboutAPRA/Publications/Pages/default.aspx >.

APRA 2013a, *Prudential Standard APS 115* Capital Adequacy: Advanced Measurement Approaches to Operational Risk, APRA, Australia, viewed 09/10/2013, <http://www.apra.gov.au/adi/PrudentialFramework/Pages/prudential-standards-and-guidance-notes-for-adis.aspx>.

APRA 2013b, *Prudential Standard APS 114* Capital Adequacy: Standardised Approach to Operational Risk, APRA, Australia, viewed 09/10/2013, <http://www.apra.gov.au/adi/PrudentialFramework/Pages/prudential-standards-and-guidance-notes-for-adis.aspx>.

APRA 2013c, *Prudential Standard APS-001*, Definitions, APRA, Australia, viewed 22/03/2014, <http://www.apra.gov.au/adi/PrudentialFramework/Documents/120928-APS-001_FINAL.pdf>.

Australian Government 1959, *Banking Act 1959 Act No. 6 of 1959 as amended*, 1, Office of Legislative Drafting and Publishing, Canberra, Legislation, <http://www.apra.gov.au/adi/Documents/cfdocs/Requirements-for-ADIs.zip>.

Australian Government Comcover, *AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines*, 2010, Comcover, Australian Government, Australia, <http://www.finance.gov.au/sites/default/files/COV_216905_Risk_Management_Fact_Sheet_FA3_23082010_0.pdf>.

Australian Trade Commission, *Australia's Banking Industry*, 2011, Austrade, Australian Government, Australia, <http://www.austrade.gov.au/ArticleDocuments/2792/Australias-Banking-Industry.pdf.aspx>.

Barney, J, Wright, M & Ketchen, DJ 2001, 'The resource-based view of the firm: Ten years after 1991', *Journal of Management*, vol. 27, no. 6, pp. 625-41.

Basel Committee on Banking Supervision 2004, *International convergence of capital measurement and capital standards - A revised framework*, The Bank for International Settlements, Basel Committee Publications, Basel, Switzerland, <http://www.bis.org/publ/bcbs107.htm>.

Basel Committee on Banking Supervision 2005, *Outsourcing in Financial Services*, The Joint Forum, Basel Committee Publications, Basel, Switzerland, <http://www.bis.org/publ/bcbs107.htm>.

Basel Committee on Banking Supervision 2011a, *Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches*, Basel Committee on Banking Supervision, Basel Committee Publications, Basel, Switzerland, <http://www.bis.org/publ/bcbs107.htm>.

Basel Committee on Banking Supervision 2011b, *Principles for the Sound Management of Operational Risk*, Basel Committee on Banking Supervision, Basel Committee Publications, Basel, Switzerland, <http://www.bis.org/publ/bcbs107.htm>.

Beaumont, N & Costa, C 2002, 'Information Technology Outsourcing in Australia', *Information Resources Management Journal*, vol. 15, no. 3, pp. 14-31.

Benit, Y, Bernstein, E, Cipolla, J & Norcio, R 2010, 'Impact of Offshore Outsourcing on Competitive Advantage of U.S. Multinational Corporations', *Journal of multidisciplinary research (Miami Gardens, Fla.)*, vol. 2, no. 2, pp. 27-52.

Bennet, M 2012, , 'You can bank on rise in IT offshoring', *The Australian*, viewed 15/04/2013 <http://www.theaustralian.com.au/business/financial-services/you-can-bank-on-rise-in-it-offshoring/story-fn91wd6x-1226294069527>

Bennett, A 2012, *Technology in Focus*, CBA, Australia,<https://www.commbank.com.au/about-us/shareholders/pdfs>.

Budd, H 2011, 'Deja vu for Commonwealth Bank customers as online banking system crashes', *The Daily Telegraph*, 15/12/2011, p. 5.

Bunyaratavej, K, Doh, J, Hahn, ED, Lewin, AY & Massini, S 2011, 'Conceptual Issues in Services Offshoring Research: A Multidisciplinary Review', *Group & Organization Management*, vol. 36, no. 1, pp. 70-102.

CBA 1997, *Annual Report1997*, Australia,<http://www.commbank.com.au/about-us/shareholders/financial-information/annual-reports.html>.

CBA 2009, *Annual Report 2009*, Australia,<http://www.commbank.com.au/about-us/shareholders/financial-information/annual-reports.html>.

CBA 2010, *Annual Report 2010*, Australia,<http://www.commbank.com.au/about-us/shareholders/financial-information/annual-reports.html>.

CBA 2011a, *Core Banking Modernisation*, CBA, Australia,<https://www.commbank.com.au/about-us/shareholders/pdfs/2011-asx/Core-Banking-Modernisation-Presentation.pdf>.

CBA 2011b, *Annual Report 2011*, Australia,<http://www.commbank.com.au/about-us/shareholders/financial-information/annual-reports.html>.

CBA 2012, *Annual Report 2012*, Australia,<http://www.commbank.com.au/about-us/shareholders/financial-information/annual-reports.html>.

CBA 2013, *Annual Report 2013*, Australia,<http://www.commbank.com.au/about-us/shareholders/financial-information/annual-reports.html>.

Chadee, D & Raman, R 2009, 'International outsourcing of information technology services: review and future directions', *International Marketing Review*, vol. 26, no. 4/5, pp. 411-38.

Coase, R 1998, 'The New Institutional Economics', *The American Economic Review*, vol. 88, no. 2, pp. 72-4.

Collins, P & Grimes, S 2011, 'Cost-competitive places: shifting fortunes and the closure of Dell's manufacturing facility in Ireland', *European Urban and Regional Studies*, vol. 18, no. 4, pp. 406-26.

Connor, G & O'Kelly, B 2012, 'Sliding Doors Cost Measurement: The Net Economic Cost of Lax Regulation of the Irish Banking Sector', *World economy*, vol. 35, no. 10, pp. 1256-76.

Dibbern, J, Goles, T, Hirschheim, R & Jayatilaka, B 2004, 'Information systems outsourcing: a survey and analysis of the literature', *SIGMIS Database*, vol. 35, no. 4, pp. 6-102.

Durie, J & Gluyas, R 2009, 'Four Pillars policy our shield against crisis', *The Australian*.

Eisenhardt, KM 1989, 'Agency Theory: An Assessment and Review', *Academy of Management Review*, vol. 14, no. 1, pp. 57-74.

Flinders, K 2014, *Why IT outsourcing is increasingly blamed for IT failures at banks*, Tech Target, viewed 17/03/2014.

Foo, F 2011, 'Westpac systems offline after back-up plan ditched', *The Australian*, 06/05/2011, p. 6.

Gartner 2013, *IT Services*, Gartner, viewed 19/03/2014, <http://www.gartner.com/it-glossary/it-services>.

Guthrie, J, Petty, R, Yongvanich, K & Ricceri, F 2004, 'Using content analysis as a research method to inquire into intellectual capital reporting', *Journal of Intellectual Capital*, vol. 5, no. 2, pp. 282-93.

Hätönen, J & Eriksson, T 2009, '30+ years of research and practice of outsourcing – Exploring the past and anticipating the future', *Journal of International Management*, vol. 15, no. 2, pp. 142-55.

Herath, T & Kishore, R 2009, 'Offshore Outsourcing: Risks, Challenges, and Potential Solutions', *Information Systems Management*, vol. 26, no. 4, pp. 312-26.

Jahns, C, Hartmann, E & Bals, L 2006, 'Offshoring: Dimensions and diffusion of a new business concept', *Journal of Purchasing and Supply Management*, vol. 12, no. 4, pp. 218-31.

Kedia, BL & Mukherjee, D 2009, 'Understanding offshoring: A research framework based on disintegration, location and externalization advantages', *Journal of World Business*, vol. 44, no. 3, pp. 250-61.

Kirkegaard, JF 2008, 'Offshoring, Outsourcing and Production Relocations — Labor Market Effects in the OECD and Developing ASIA', *The Singapore Economic Review*, vol. 53, no. 3, pp. 371-418.

KPMG 2014, *Managing risk and complexity* KPMG, viewed 18/05/2014, <http://www.kpmg.com/au/en/topics/managing-risk-complexity/Pages/default.aspx>.

Krippendorff, K 2013, *Content Analysis An Introduction to Its Methodology*, Third edn, SAGE Publications, Inc., United States of America.

Lacity, MC, Khan, SA & Willcocks, LP 2009, 'A review of the IT outsourcing literature: Insights for practice', *The Journal of Strategic Information Systems*, vol. 18, no. 3, pp. 130-46.

Laker, J 2008, 'Basel II – Observations from Down Under', *Financial Markets, Institutions & Instruments*, vol. 17, no. 1, pp. 31-42.

Lane, MS & Van der Vyver, G 2006, 'Does off-shoring IT make good business sense? Proceed with caution!', in 10th Pacific Asia Conference on Information Systems (PACIS 2006): *proceedings of the10th Pacific Asia Conference on*

Information Systems (PACIS 2006), B Tan (ed.), Kuala Lumpur, Malaysia, <http://eprints.usq.edu.au/3411/>.

Laurent, W 2006, 'Outsourcing Governance', *DM Review*, vol. 16, no. 10, pp. 14-5.

Lee, CKM, Yeung, YC & Hong, Z 2012, 'An integrated framework for outsourcing risk management', *Industrial Management & Database Systems*, vol. 112, no. 4, pp. 541-58.

Mathew, SK & Chen, Y 2013, 'Achieving offshore software development success: An empirical analysis of risk mitigation through relational norms', *The Journal of Strategic Information Systems*, vol. 22, no. 4, pp. 298-314.

Mestchian, P 2012, *Run the bank vs Change the bank*, Chartis Research, viewed 22/03/2014, <http://risktech-forum.com/opinion/run-the-bank-vs-change-the-bank>.

Moosa, I 2011, 'Operational risk as a function of the state of the economy', *Economic Modelling*, vol. 28, no. 5, pp. 2137-42.

Newman, R 2013, *Commonwealth Banks*, Nine News, viewed 18/03/2014, <http://finance.ninemsn.com.au/newsbusiness/motley/8704858/commonwealth-will-not-offshore-jobs>.

Ørberg Jensen, PD & Pedersen, T 2011, 'Offshoring and international competitiveness: antecedents of offshoring advanced tasks', vol. 40, no. 2, pp. 313-28.

Palugod, N & Palugod, PA 2011, 'Global Trends in Offshoring and Outsourcing', *International Journal of Business & Social Science*, vol. 2, no. 16, pp. 13-20.

PwC 2014, *Financial Services Regulation*, PwC, viewed 18/05/2014, <http://www.pwc.com.au/industry/financial-services-regulation/index.htm>.

Raman, R & Chadee, D 2007, 'Offshoring of IT services: a survey of the literature and towards a new research agenda', in Australian and New Zealand International Business Academy (ANZIBA) 2007: *proceedings of theAustralian and New Zealand International Business Academy (ANZIBA) 2007*, FG Rose E. L. (ed.), CD ROM, Newcastle, Australia, pp. 1-24.

Roza, M, Van den Bosch, FAJ & Volberda, HW 2011, 'Offshoring strategy: Motives, functions, locations, and governance modes of small, medium-sized and large firms', *International Business Review*, vol. 20, no. 3, pp. 314-23.

Scardino, L, Anderson, DS, Brown, RH, Da Rold, C, Dreyfuss, C, Karamouzis, F, Lovelock, J-D, Maurer, W, Moore, C & Young, A 2005, 14/12/2005, 'Gartner on Outsourcing', *Gartner on Outsourcing, 2005*, pp. 1-42,

Simon, JC, Poston, RS & Kettinger, B 2009, 'Creating Better Governance of Offshore Services', *Information Systems Management*, vol. 26, no. 2, pp. 110-22.

Smith, P 2002, 'Australian IT Directors Manage thier Vendors Relationships', *MIS Australia*, January 2003, pp. 31-6.

Srivastava, SC & Teo, TSH 2012, 'Contract Performance in Offshore Systems Development: Role of Control Mechanisms', *Journal of Management Information Systems*, vol. 29, no. 1, pp. 115-58.

Stemler, S 2001, 'An Overview of Content Analysis', *Practical assessment, research & evaluation*, vol. 7, no. 17.

Stratman, JK 2008, 'Facilitating offshoring with enterprise technologies: Reducing operational friction in the governance and production of services', *Journal of Operations Management*, vol. 26, no. 2, pp. 275-87.

Strijbos, J-W, Martens, RL, Prins, FJ & Jochems, WMG 2006, 'Content analysis: What are they talking about?', *Computer & Education*, vol. 46, no. 1, pp. 29-48.

Tait, V 2012, *CBA rejects need to send jobs offshore*, Morning Star, viewed 18/03/2014, <http://www.morningstar.com.au/stocks/article/rejects-need-to-send-jobs-offshore/4702>.

Tate, WL, Ellram, LM, Bals, L & Hartmann, E 2009, 'Offshore outsourcing of services: An evolutionary perspective', *International Journal of Production Economics*, vol. 120, no. 2, pp. 512-24.

Terry, C 2009, 'The New Basel Capital Accord: A Major Advance at a Turbulent Time', *Agenda: A Journal of Policy Analysis and Reform*, vol. 16, no. 1, pp. 25-43.

WBC 2009, *2009 Annual Report*, Westpac Banking Corporation, Australia,<http://www.westpac.com.au/about-westpac/investor-centre/annual_reports/>.

WBC 2010a, *2010 Annual Report*, Westpac Banking Corporation, Australia,<http://www.westpac.com.au/about-westpac/investor-centre/annual_reports/>.

WBC 2010b, *The Westpac Group IT & Productivity Update*, WBC, Australia,<http://www.westpac.com.au/docs/pdf/aw/ic/101008_IT_and_Productivity_Final.pdf>.

WBC 2011, *2011 Annual Report*, Westpac Banking Corporation, Australia,<http://www.westpac.com.au/about-westpac/investor-centre/annual_reports/>.

WBC 2012, *2012 Annual Report*, Westpac Banking Corporation, Australia,<http://www.westpac.com.au/about-westpac/investor-centre/annual_reports/>.

WBC 2013, *2013 Annual Report*, Westpac Banking Corporation, Australia,<http://www.westpac.com.au/about-westpac/investor-centre/annual_reports/>.

Whitaker, J, Mithas, S & Krishnan, MS 2010, 'Organizational Learning and Capabilities for Onshore and Offshore Business Process Outsourcing', *Journal of Management Information Systems*, vol. 27, no. 3, pp. 11-42.

Wilkinson, M 2006, 'Designing an 'adaptive' enterprise architecture', *BT Technology Journal*, vol. 24, no. 4, pp. 81-92.

Willcocks, L 2011, 'Machiavelli, management and outsourcing: still on the learning curve', *Strategic Outsourcing: An International Journal of Business & Social Science*, vol. 4, no. 1, pp. 5-12.

Willcocks, LP, Lacity, MC & Kern, T 1999, 'Risk mitigation in IT outsourcing strategy revisited: longitudinal case research at LISA', *The Journal of Strategic Information Systems*, vol. 8, no. 3, pp. 285-314.

Yeates, C 2013, 'Westpac jobs to stay for now: Kelly', *The Sydney Morning Herald*, 08/03/2013.