FINANCIAL SUPPLY CHAIN RISK IN AUSTRALIAN
FINANCIAL INSTITUTIONS

A thesis submitted in fulfilment of the requirements for the degree of Doctor of Philosophy

Ibrahim Abdallah
BSC (Information Technology), Eastern Mediterranean University, Cyprus
M. Banking and Finance, Eastern Mediterranean University, Cyprus
M. Accounting, Victoria University, Australia
MBA, Monash University, Australia

School of Business IT and Logistics, College of Business
RMIT University

June 2019
DECLARATION

I certify that, except where due acknowledgement has been made, the work is that of the author alone; the work has not been submitted previously, in whole or in part, to qualify for any other academic award; the content of the thesis is the result of work which has been carried out since the official commencement date of the approved research program; any editorial work, paid or unpaid, carried out by a third party is acknowledged; and ethics procedures and guidelines have been followed.

I acknowledge the support I have received for my research through the provision of an Australian Government Research Training Program Scholarship.

Ibrahim Abdallah
June 2019
DEDICATION

This thesis is dedicated to Dr Asmah Abdallah, and my parents, Nawal Abdallah and Abdalkhaleq Abdallah, for their support and encouragement.
ACKNOWLEDGEMENTS

I would like to extend my appreciation to my supervisors for their patience, valuable advice and support, Professor Shams Rahman and Dr Kamul Ahsan.

Grateful thanks to those who have assisted me throughout my research and the writing of this thesis, including friends, colleagues and RMIT staff, especially Dr Huan Vo-Tran and Dr Vince Bruno, who provided support, encouragement and advice.

Many thanks also to the research participants, the senior management of the banks who facilitated the study in their financial institutions, and an editor who helped with proof reading and grammar.

My thanks go to several people who also provided support and assistance, including David Thompson, Steve Whiteling and Austen Burleigh.
TABLE OF CONTENTS

DECLARATION........................................................................................................................... II
DEDICATION ............................................................................................................................. III
ACKNOWLEDGEMENTS ......................................................................................................... IV
TABLE OF CONTENTS .......................................................................................................... V
LIST OF FIGURES.................................................................................................................. XII
LIST OF TABLES .................................................................................................................... XIV
ABBREVIATIONS .................................................................................................................. XV
ABSTRACT ........................................................................................................................... XVIII
CHAPTER 1 INTRODUCTION ................................................................................................. 1
1.1 Introduction ........................................................................................................ 1
1.2 Background ......................................................................................................... 2
1.3 Problem identification ........................................................................................ 4
1.4 Research rationale .............................................................................................. 7
1.5 Research objectives and questions ..................................................................... 8
1.6 Methodology ....................................................................................................... 8
  1.6.1 Multi-case study design ....................................................................................... 8
  1.6.2 Conceptual framework development ................................................................. 9
  1.6.3 Current state analysis ...................................................................................... 10
  1.6.4 Future state analysis ....................................................................................... 10
1.7 Scope of the research ........................................................................................ 11
1.8 Contribution of the research ............................................................................. 11
3.2 Research paradigm ........................................................................................................ 70

3.3 Methodology ................................................................................................................. 73

3.3.1 Qualitative multi-case studies ....................................................................................... 74

3.3.2 Analysis method: thinking process of the theory of constraints .................................. 78

3.3.3 Description of the application of TP methods to the case studies ......................... 80

3.3.3.1 The thinking process as an analytic tool ................................................................. 81

3.3.3.2 Identification of the undesirable effects ................................................................. 82

3.3.3.3 Current reality tree construction process method .................................................. 84

3.3.3.4 Future reality tree construction process method .................................................... 86

3.3.3.5 Steps in preparing the future reality tree ............................................................... 88

3.4 Data collection procedures ......................................................................................... 93

3.4.1 Data collection sample ............................................................................................... 93

3.4.1.1 National Australia Bank ......................................................................................... 95

3.4.1.2 Bendigo and Adelaide Bank ................................................................................... 95

3.4.1.3 MyState Bank ....................................................................................................... 96

3.4.1.4 Sample selection .................................................................................................... 96

3.4.3 Interview protocol ..................................................................................................... 97

3.4.4 Interview procedures and schedule ........................................................................... 100

3.5 Interview inquiry and the research process ................................................................. 103

3.5.1 Reliability and validity ............................................................................................. 106

3.5.2 Ethical and critical reflections ................................................................................... 109

3.6 Summary ...................................................................................................................... 110
CHAPTER 4 ANALYSIS AND RESULTS: CURRENT STATE ANALYSIS ..............................................111

4.1 Introduction ..................................................................................................................111

4.2 Financial institutions in Australia ..............................................................................112

4.2.1 Operations level ......................................................................................................115

4.2.2 Business strategy level ..........................................................................................115

4.2.3 Corporate strategy level .......................................................................................116

4.3 Current state analysis ...............................................................................................117

4.3.1 Current reality tree for demand in retail banking ..................................................119

4.3.2 Current reality tree for supply in business banking ...............................................127

4.3.3 Current reality tree for product management .........................................................134

4.3.4 Current reality tree for information technology ......................................................139

4.3.5 A combined current reality tree for the entire organisation ....................................147

4.3 Summary ....................................................................................................................159

CHAPTER 5 ANALYSIS AND RESULTS: FUTURE STATE ANALYSIS ................................161

5.1 Introduction ................................................................................................................161

5.2 Risk treatments: injections .......................................................................................162

5.2.1 Operations level related injections ......................................................................164

5.2.1.1 Operations injection 1: Operations actions .........................................................164

5.2.1.2 Operations injection 2: Operations assessment ..................................................165

5.2.1.3 Operations injection 3: Operations control centre ..............................................165

5.2.1.4 Operations injection 4: Operations risk register ................................................166

5.2.1.5 Operations injection 5: Operations monitoring and reporting centre ................166

5.2.1.6 Operations injection 6: Operations risk library ................................................166
LIST OF FIGURES

Figure 1.1 Overview of thesis structure ....................................................................................... 16
Figure 2.1 Proposed conceptual model of FSCR factor types ........................................................... 54
Figure 3.1 Illustration of the identification and perceived causes of undesirable effects and identifying the ‘what to change’ part of the TP method ............................................................... 83
Figure 3.2 Example of a CRT showing the undesirable effects that collectively cause a core problem ........................................................................................................................................... 87
Figure 3.3 Use of an injection or solution in future reality trees to convert causes of undesirable effects into desirable effects ........................................................................................................ 89
Figure 3.4 Illustration of the future reality tree (FRT) showing locations of injections (solutions) to create desirable effects (DEs) ............................................................................................................ 91
Figure 3.5 The research analysis process summarised as first CRT construction, followed by FRT construction and the use of the FRT and injections in risk management plan implementation ........................................................................................................................................ 92
Figure 3.6 Overview of the research process ............................................................................... 105
Figure 4.1 Generalised financial institution structure .................................................................... 114
Figure 4.2 Current reality tree for demand in retail banking ........................................................... 121
Figure 4.3 Current reality tree for supply in business banking ....................................................... 130
Figure 4.4 Current reality tree for product management ............................................................... 136
Figure 4.5 Current reality tree for information technology ........................................................... 142
Figure 4.6 Combined current reality tree for the entire organisation ............................................. 148
Figure 4.7 Summary of the identified risks mapped to financial institution functional structure ................................................................................................................................. 158
Figure 5.1 Future reality tree for demand in retail banking ............................................................. 174
LIST OF TABLES

Table 2.1 Examples of supply chain risk definitions ................................................................. 20
Table 2.2 Summary of supply chain risk types ........................................................................ 22
Table 2.3 Examples of supply chain risk classifications .......................................................... 23
Table 2.4 Definitions of FSCR ................................................................................................. 32
Table 2.5 Contributions regarding FSCR management ............................................................ 34
Table 2.6 Summary list of demand risk factors in the supply chain ........................................ 37
Table 2.7 Summary list of supply risk factors in the supply chain ........................................... 40
Table 2.8 Supply risk examples ............................................................................................... 41
Table 2.9 Banks with the greatest all-cause losses ................................................................... 48
Table 2.10 Summary list of potential sources of risk discussed in earlier sections ................. 55
Table 2.11 Studies of the application of the theory of constraints in various service sector types .................................................................................................................................. 61
Table 3.1 Summary of the thinking process core questions, purposes and analysis tools .......... 81
Table 3.2 Description of participants ....................................................................................... 97
Table 4.1 Contributing CRT elements to demand in retail banking core risk effects ............. 127
Table 4.2 Contributing CRT elements to supply in business banking core risk effects .......... 133
Table 4.3 Contributing CRT elements to product management core risk effects ................. 140
Table 4.4 Contributing CRT elements to IT core risk effects .................................................. 146
Table 4.5 Main underlying core risk effect types .................................................................... 155
Table 6.1 Summary of undesired effects contributing to underlying core risk effect types ....... 210
Table 6.2 Classification of injections with supply chain risk management process typology ... 215
## ABBREVIATIONS AND DEFINITIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ANZ</strong></td>
<td>Australia and New Zealand Banking Group Limited</td>
</tr>
<tr>
<td><strong>APRA</strong></td>
<td>Australian Prudential Regulation Authority</td>
</tr>
<tr>
<td><strong>ATM</strong></td>
<td>Automated Teller Machine</td>
</tr>
<tr>
<td><strong>BOQ</strong></td>
<td>Bank of Queensland</td>
</tr>
<tr>
<td><strong>CBA</strong></td>
<td>Commonwealth Bank of Australia</td>
</tr>
<tr>
<td><strong>CCR</strong></td>
<td>Capacity-constrained resource</td>
</tr>
<tr>
<td><strong>CIT</strong></td>
<td>Cash in transit</td>
</tr>
<tr>
<td><strong>CRT</strong></td>
<td>Current reality tree</td>
</tr>
<tr>
<td><strong>DBR</strong></td>
<td>Drum-buffer-rope</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>DE</td>
<td>Desirable effect</td>
</tr>
<tr>
<td>EFTPOS</td>
<td>Electronic Funds Transfer at Point of Sale</td>
</tr>
<tr>
<td>FRT</td>
<td>Future reality tree</td>
</tr>
<tr>
<td>FSC</td>
<td>Financial supply chain</td>
</tr>
<tr>
<td>FSCR</td>
<td>Financial supply chain risk</td>
</tr>
<tr>
<td>FSCRM</td>
<td>Financial supply chain risk management</td>
</tr>
<tr>
<td>IT</td>
<td>Information technology</td>
</tr>
<tr>
<td>M2M</td>
<td>Machine to machine</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
</tr>
<tr>
<td>NAB</td>
<td>One of the four largest deposit taking financial institutions in Australia in terms of market capitalisation, earnings and customers.</td>
</tr>
<tr>
<td>ODM</td>
<td>A planning methodology used to forecast, plan for and manage the operations organised to meet the demand for products and services.</td>
</tr>
<tr>
<td>OPT</td>
<td>A production scheduling and inventory control system that aims to simultaneously raise throughput while reducing inventory and operating costs, and achieve a smooth, continuous flow of work in process.</td>
</tr>
<tr>
<td>RQ</td>
<td>An objective of an investigation of an issue to be examined through the application of methods of rational inquiry.</td>
</tr>
<tr>
<td>TOC</td>
<td>A management philosophy that views any manageable system as being limited in achieving more of its goals by a very small number of constraints.</td>
</tr>
<tr>
<td>TP</td>
<td>The thinking processes in the theory of constraints are methods to enable the focused improvement of any system (especially organisational systems).</td>
</tr>
<tr>
<td>UDE</td>
<td>A theory of constraints concept, visually depicted in current reality trees. It represents the perceived undesirable effects of a small number of root causes, the constraints.</td>
</tr>
<tr>
<td>VAR</td>
<td>A measure of the risk of loss for investments. It estimates how much a set of investments might lose, given normal market conditions, in a set time period.</td>
</tr>
</tbody>
</table>
ABSTRACT

The management of financial supply chain risks (FSCR) in financial institutions is important for their performance. FSCR are defined as financial institution risk effects viewed from a supply chain perspective that constrain attainment of institutional objectives. With limited research on FSCR in the context of financial institutions, the literature identifies a need for holistic research that advances understanding of how risk factors operate jointly rather than in isolation. To contribute to addressing these issues, this research examines FSCR in Australian financial institutions. A conceptual model of FSCR was developed and the research used the thinking process (TP) of the theory of constraints (TOC). The methods of TP, such as the current reality tree (CRT) and the future reality tree (FRT), are employed respectively to investigate the existing situation and to propose alternatives. These methods can accommodate the examination of multiple FSCR factors jointly from the perspective of an organisation in its entirety. The case study participants comprised nine senior risk management participants, three from each of three Australian financial institutions. The institutions represented each of three Australian deposit-taking capitalisation tiers: large, medium and small.

The current state of financial institution risk causation was depicted in CRT maps aggregated from the three cases. CRTs mapped the most influential core effects contributing to risk. The results showed that the most influential risk core effect types comprised people-centred failures, external service provider disruptions, policy and regulatory compliance limitations, and technology hub failures. The results also showed the causal risk pathways arising from these effects as risk moved dynamically among the operational level, business strategy level and corporate strategy level of the financial institutions and across the major business types, comprising retail financial services,
wholesale and business financial services, product management and enterprise information technology services and management.

The TP FRT method was applied to depict a desired future, with a comprehensive range of complementary risk management system initiatives modelled. This was to simulate the conversion of the current state undesired effects (UDEs) identified in the CRT analysis into desired effects (DEs). This comprised an interconnected system of risk controls, including an enterprise network of risk monitoring, risk assessment and analysis, and mitigation solutions. A finding was that effectiveness was dependent on the strength of interconnectedness of the risk control elements across the organisation in its entirety.

This research showed that an entire organisation perspective provided by the application of TP methods to Australian financial institutions has both theoretical and practical implications. The theoretical implications are that TP methods used in this research facilitate a comprehensive examination of financial institution risk from a supply chain perspective that encompasses an entire organisational view. First, multiple risks were jointly identified and mapped together to provide an entire organisational view. Second, the relative importance of the risks for explaining business disruption was evaluated. Third, the interrelationships among the risks and the pathways of risk movement through the institutions were identified and the interconnected nature of risk processes demonstrated. The application of TP methods to FSCR in this research contributed to the better understanding of the nature of risk in financial institutions. A theoretical implication is that rather than portraying risk as arising from a discrete subset of variables and manifesting in isolation, the results revealed the complexity of supply chain risk determinism in Australian financial institutions, such that risk causal pathways were found to be interconnected and crossed over organisational functions and structures.
Informed by this comprehensive examination of risk from a perspective that encompasses the entire organisation, the dependencies among risk management phases and approaches that were demonstrated also contributes to a better understanding of interconnectedness among risk factors relevant to the consideration of risk mitigation effectiveness. The FRT analyses illustrated the practical contribution of the results, where applied risk controls simulated the effectiveness of risk mitigation. In practice, the risk mitigation implementation approach is recommended to be highly interconnected and comprehensively managed as an interacting system of risk controls. The research was a novel application of TP methods from a supply chain perspective to examine risk and risk mitigation in Australian financial institutions. A limitation of the research is qualified generalisability to other financial institutions, especially those with different service mixes. Also, international generalisability may be limited by the Australian context because of regulatory environment differences.

**Keywords:** risk assessment, financial institutions, theory of constraints, current reality tree, future reality tree, banking, supply chain, supply chain risk, financial supply chain risk
CHAPTER 1

INTRODUCTION

1.1 Introduction

This research examines the causes of financial supply chain risks (FSCR) in Australian financial institutions. Adapted from Ho et al. (2015), FSCR in this research is defined as the likelihood and impact of unexpected macro- and/or micro-level financial-related effects or conditions that adversely influence any aspect of a supply chain and constrain operational, tactical or strategic attainment in financial institutions. Based on a review of the literature, a conceptual model of the determinants of FSCR was developed. A generic model of Australian financial institution functions and structure was constructed from aggregated participant information. Guided by these models, the nature and operation of FSCR were examined in a whole-of-organisation current state analysis of aggregated multi-case study data to identify the most influential contributing risk factors. A future state analysis was then undertaken to provide a whole-of-organisation perspective on how a set of risk remediation elements might work together in a comprehensive and coordinated solution approach to managing financial institution risks. The findings of this study extend what is known about FSCR determinants and mitigation, taking into account the complexity in Australian financial institution risk dynamics.

This chapter provides a brief introduction to the research. Section 1.2 presents background information about organisational financial risks. In Section 1.3, problem identification is described, while Section 1.4 reviews the preliminary literature and outlines the research rationale of the study. The objectives of the research and the specific research questions are proposed in Section 1.5. A brief overview of the methodology adopted in this study is given in Section 1.6,
while Section 1.7 describes the scope of the research. The theoretical and practical contributions of the study are stated in Section 1.8. Section 1.9 outlines the subsequent chapters, and finally, a summary of the thesis is provided in Section 1.10.

1.2 Background

The management of supply chain risks (SCR) in organisations is critical to avoid financial loss and improve organisational performance (Babich & Kouvelis 2018; Ivanov Sokolov & Dolgui 2014; Ivanov et al. 2017). A supply chain view of risk considers the whole organisational operating environment context, as well as discrete organisational characteristics. It refers to all business practices that are assimilated for the purpose of the provision of services and products required by consumers (Harland 1996; Cousins et al. 2008.

While no agreed definition exists, authors have stressed the multifaceted and complex nature of SCR (Fan & Stevenson 2018; Ho et al. 2015; Sohdi, Son & Tang 2012). Ho et al. (2015), in a systematic review of the literature, provided a comprehensive and inclusive definition (p. 5035) of supply chain risk:

the likelihood and impact of unexpected macro and/or micro level effects or conditions that adversely influence any part of a supply chain leading to operational, tactical, or strategic level failures or irregularities.

In this research, FSCR utilises Ho et al.’s (2015) definition, adapted to include operational financial effects or conditions as they might apply in financial institution organisations. FSCR concerns the examination of financial-related risk from a supply chain perspective with impacts on the operations of financial institutions. The effect of environmental financial disruptions from systemic macro-economic risks cannot be ignored in the financial industry sector; however, the
scope of this study is concerned with controllable risks that adversely affect financial institutions operations, from a supply chain perspective. In financial institutions, it is expected that most aspects of supply chain risk are either directly or indirectly financially related in some way, as the nature of their business is inherently financial.

Ellram, Bals and Tate (2018) highlighted the importance of SCR, arguing they significantly influence competitiveness and organisational viability. According to a survey carried out by the Association of Financial Professionals (2014), 90% of respondents indicated that risk management was strategically important. The survey also showed that 84% of respondents indicated that their organisations currently had increased exposure to risk than in the previous three years. Organisations, including banks, have strategically used investments and other financial techniques to indirectly offset potential losses as an approach to manage SCR (Cole & Ji 2018; Ziman 2013). For instance, a number of studies of American companies showed that over 60% employed derivative contract techniques (e.g., Wuttke, Blome & Henke 2013) to manage risk of future financial losses. Viswanadham and Samvedi (2013) indicated that up to 90% of large firms in the UK used derivatives to manage risk of financial loss, as do banks in Australia (Cole & Ji 2018). Monitoring data from the Bank for International Settlements showed increases in hedging investment (Sodhi, Son & Tang 2012). Even with the increased use of derivative contract techniques, over the years, the increase in SCR has continued (Sodhi, Son & Tang 2012). However, there is limited research to provide guidance about direct assessment, mitigation and recovery from the impact of SCR on financial institutions (Ivanov et al. 2017).

Despite the importance of financial-related risks from a supply chain perspective on financial institution risk, the literature review in Chapter 2 found that FSCR in financial institutions has been subject to limited examination. This research investigates FSCR in a sample of three
Australian deposit-taking financial institutions, comprising one with large capitalisation, one medium and one small (Gorajek & Turner 2010). Next, information on the impacts of risk is reviewed.

1.3 Problem identification

Supply chains are considered the backbone of the international economy (Malaket 2013, 2014). Organisational risk of financial loss can result from multiple factors in the supply chain (Jereb, Cvahte & Rosi 2012). The supply chain refers to all business practices that are assimilated for the purpose of the provision of services and products required by consumers (Harland 1996; Ho et al. 2015). In particular, the financial-related aspects of supply chains are an essential part of business operations, and this is particularly so for financial institutions where the product is comprised of some aspect of money, and the services involve the movement of money through a network of transactional processes in the supply chain. The transaction process system comprises devices, databases, procedures and people (Stair & Reynolds 2010). For example, banks and their technology infrastructure service providers risk manage the machine-to-machine (M2M) networks comprising Automated Teller Machines (ATMs) and Electronic Funds Transfer at Point of Sale technologies (EFTPOS) (Tuna et al. 2017). To mitigate the probability of loss, FSCR management (FSCRM) refers to those components, procedures, technologies, techniques or treatments that are applied to a FSC to reduce risk of loss (Stair & Reynolds 2010).

FSCR can also result from interorganisational relationships (Wallenburg et al. 2011; Blijleven et al. 2018). For example, historically, business organisations requiring working capital and liquidity for the purpose of supporting operations worked independently of trading partners and sought this capital on the basis of their own requirements (Manuj & Mentzer 2008). Often, companies had goals that were in conflict with those of their trading partners. While buyer firms attempted to
procure additional inventory with extended terms of payment, resulting in a rise in revenues, the supplier firms sought to reduce the selection period (Machowiak 2012). To sustain growth in business and to compete in a volatile economy, firms have sought collaborative methods via which to improve their working capital and liquidity (Liu, Anderson & Cruz 2012). By emphasising business flows that include only buyers that are highly rated, and other methods, financial risk from partner organisations can be mitigated (Jereb, Cvahte & Rosi 2012).

To remain competitive in the market, financial institutions require the necessary adaptive skills to reduce supply chain risks, where exposure to even one component of such FSCR can render the entire system unstable (Park 2012). As deposit-taking institutions in Australia have expanded, a number of technology-related risks have emerged in the supply chain; for example, disruptions caused by technology cause system disruptions to financial transaction processes (Withers 2018). Risk exposure can disrupt the flow of FSC management in financial organisations, as encountered in daily operations (Handfield & Nichols 1999; Ho et al. 2015; Fan & Stevenson 2018).

As business competition has increased, FSCR management has become a focus for financial institutions internationally, as reducing risk creates a competitive advantage over other financial institutions in similar markets (Dyckman 2011). The availability of techniques for FSCR management in Australian financial industries to combat financial supply chain vulnerability and risks remains an issue of industry concern. For example, over 70% of corporate treasury and finance professionals are hesitant about adopting mobile payments at their organisations, as they question the security of this payment method (Association for Financial Professionals 2017).

Financial loss risk from the FSC is a major issue for Australian financial institutions. The more visible FSCR includes theft, forgery and hacking (Association for Financial Professionals 2017). In 2017, as Australian consumers spent more than ever on cards, the overall value of card
transactions grew 5% from 2016, to $748.1 billion. The value of fraudulent transactions grew in line with this total, also increasing 5% to $561.4 million from 2016 to 2017 (Australian Payments Network 2018).

There is a trend of worsening impact of financial transaction risks—fraud related to Australian payment card transactions has more than doubled from 32 cents per A$1000 in 2008 to 75 cents in 2017 (Australian Payments Network 2018). This shows an increase in the card fraud rate is commensurate with the growth in electronic payment card use in Australia (Australian Payments Network 2018). Further, there has been an increasing trend in debit card transaction fraud from 2008. Fraud through card skimming or counterfeit cards has the highest value compared with other fraud incidents, accounting for about 80% of all fraud involving debit cards alone (Australian Payments Network 2018).

In addition to the cost impact of transaction risks illustrated above, recent effects concerning financial institution risk has received considerable public attention in the Australian media. These include the establishment of the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry in 2017 (Commonwealth of Australia 2018, 2019). Risk of reputation loss and customer dissatisfaction is shown in the interim report, where the report’s executive summary (p. 1) found that ‘conduct by financial services entities that has brought public attention and condemnation’, and where ANZ, BOQ, CBA, Macquarie Bank, NAB and Westpac all acknowledged misconduct. Another example of FSCR is technology services provider failures causing major disruptions; for example, the Australian provider of network services caused a national outage that left many bank customers unable to use EFTPOS or ATMs, leading to nationwide retail and other business disruptions (Withers 2018).
1.4 Research rationale

There is a lack of comprehensive and in-depth research on FSCR and risks in financial institutions (Ho et al. 2015; Fan & Stevenson 2018). In addition, in relation to SCR in general (Kim, Mabin & Davies 2008), there is a lack of research that has application utility and could be adapted to more effectively mitigate FSCR. In Australia, banks comprise banking businesses as well as a range of other financial products such as insurance and investment products. For this reason, they are usually referred to as financial institutions in this thesis, but the term bank is also used where the literature refers to financial institutions as banking entities specifically.

Researchers (Ho et al. 2015; Fan & Stevenson 2018) indicate that while there is substantial research on various risk factors in the supply chain, these are often examined in isolation, with little indication of complex real-world applicability or generalisability. Consequently, supply chain risk researchers have called for more holistic examination of risk (Fan & Stevenson 2018; Ghadge et al. 2012; Gelsomino et al. 2016; Ho et al. 2015); in particular, research on the joint impact of risks could lead to better management of risk. Ho et al. (2015) suggest that field and case studies are methodologies able to accommodate research that can make sense of real-world complexity in a way that offers practical risk mitigation models and understanding. According to Ho et al. (2015), research that examines the joint impact of multiple risks has potential to assist scholars and risk practitioners to better understand the impact and control of financial risks. To address the gaps in relation to the limited research on FSCR in financial institutions and the use of methods able to accommodate a holistic perspective on FSCR, this research makes use of case study and risk analysis methods that are able to accommodate complex risk determinism in financial institutions from a supply chain perspective.
1.5 Research objectives and questions

The objective of this research is to provide an in-depth understanding of FSCR and their mitigation in Australian financial institutions. An in-depth understanding aims to identify the nature and causes of FSCR in Australian financial institutions by taking a whole-of-organisation view of FSCR from a supply chain perspective. A further aim is that this in-depth analysis provide a basis to devise approaches for mitigating the identified FSCR appropriate for practical application in Australian financial institutions.

To fulfil these objectives, the following research questions (RQ) are posed:

RQ1: What FSCR are identified as currently present in Australian financial institutions?
RQ2: What is the nature of the causal relationships among the FSCR that adversely affect financial institution business functions?
RQ3: What future risk control practices could mitigate FSCR in Australian financial institutions?

1.6 Methodology

1.6.1 Multi-case study design

A qualitative multi-case study design was adopted to achieve the aims of this research and address the research questions. The cases selected comprise three financial institutions stratified from the three tiers of Australian deposit-taking institutions (Gorajek & Turner 2010); in terms of relative capitalisation, they comprise one large (Tier 1), one medium-sized (Tier 2) and one small financial institution (Tier 3). The participant sample comprised nine participants, three from each of the three financial institution cases. The participants all occupied senior risk management roles within
the institutions, with one from each institution occupying a chief risk officer or equivalent senior risk manager role with whole-of-organisation strategic risk management role scope. The other six participants, two from each of the three institutions, were senior risk managers or analysts with more discrete role scope, but all occupying risk management specialised roles.

Case studies investigate a contemporary phenomenon within real-life context, and are well suited for exploratory and theory-building research (Eisenhardt 1989; Yin 2017). The number of cases and participants selected was judged the best balance between a multi-case design that accommodates an in-depth approach without being overwhelmed by voluminous qualitative data, and a single-case design with in-depth richness but lacking replication-based generalisability and prone to data bias and distortions (Eisenhardt 1991; Yin 2014). In-depth data suit the inductive process of FSCR causal theory building to make sense of real-world risk phenomena, and was considered more appropriate to provide an in-depth understanding of FSCR and their mitigation in Australian financial institutions.

1.6.2 Conceptual framework development

To create the context for the case studies, the literature was examined to inform the case study design. First, guided by the research questions literature related to the research was reviewed. The review of related literature informed understanding of the nature of FSCR. Such an understanding led to the development of a conceptual framework that identified what has been found to be the main risks relevant to the sample of financial institutions in the case studies. The conceptual structure provided by the framework informed the interviewing approach, making sense of the qualitative case study interview data and the formulation of the analyses.
1.6.3 Current state analysis

The qualitative multi-case research strategy comprising both interview-elicited data and the analyses was guided by a management philosophy (Watson, Blackstone & Gardiner 2006) called the theory of constraints (TOC) (Goldratt 1990). The TOC thinking process (TP) analysis methods comprising current reality trees (CRTs) were used to address the first two research questions in a current state analysis of interview data. This answered the research questions relating to the identification and nature of FSCR and the causal relationships among them in the financial institutions. The CRTs were used to map the multidetermined nature of problems called undesirable effects (UDEs) in the financial institution’s operations, and explain the underlying causes of FSCR and risk impacts on business functions.

1.6.4 Future state analysis

Guided by the results of the current state analysis, a future state analysis applied CRT maps and iteratively verified findings with the participants. This answered the third research question on future risk control practices that could mitigate FSCR in Australian financial institutions. The CRT results were used as the basis to develop future reality trees (FRTs) to model and map a desired future state where risk is effectively controlled. The application of the solutions (which in the TOC are called ‘injections’) into the organisation was explored with the participants to critically develop an applied risk management approach. Finally, the findings of the data analysis are discussed and interpreted to draw specific conclusions to adequately answer the research questions.
1.7 Scope of the research

The financial services industry is typically involved in scenarios where systemic or external risks tend to affect the whole sector, such as the global financial crisis or other macro-economic shocks. Although the effect of systemic risks cannot be ignored in the industry, the scope of this study is concerned only with internal controllable risks that affect a company’s operations. The risk effects examined include those that interact with institutional customers and suppliers in the financial supply chain. In this research, the focus is on FSCR from a supply chain perspective in Australian financial institutions.

1.8 Contribution of the research

This research contributes to the existing body of knowledge and research relating to financial institution risk in several ways, as outlined in Sections 1.8.1 and 1.8.2.

1.8.1 Contribution to theory

A major contribution of this research was the examination of risks jointly rather than in isolation from a view of an organisation in its entirety. The research utilised TOC TP methods combined with a multi-case study method in a novel approach to examining financial institution risks from a supply chain perspective. The approach was novel in that it used complex process mapping rather than simple theme description typical of case study thematic description approaches more generally. For example, the TP is capable of handling complex causal relationships between undesired effects which is usually not possible using simple case study or survey methods. Systems dynamics methods have capacity for portraying complexity but TP is more usually applied in organisational contexts that have a problem solution emphasis (Größler 2009) Furthermore, the process mapping was illustrated though whole organisation visualisations. This
approach accommodated the complexity of a whole-of-organisation perspective, and the practical application utility that such a perspective provides. Further, it revealed the dynamic and interrelated nature of risk causal pathways when risks are examined jointly and contextualised within financial institution functional and structural characteristics. It also showed that distinctions between FSCR and other non-financial SCR when applied to Australian financial institutions are not readily separable. This is both because of the intrinsic financial nature of the business of financial institutions and the dynamic and interconnected nature of risk causal pathways.

1.8.2 Contribution to practice

An objective of this research was to design strategies to manage FSCR that have potential for application in practice. The findings of the analyses contribute to a deeper understanding of the dynamics of financial institution risk, and how they can be practically implemented in a financial institution to control risk. The results show how the existing risk profile of an organisation, which is informed by the current state analysis method, could be transformed through transition to a desired future state, which is informed by the future state analysis method. The practical usability of the findings for financial institutions is facilitated by the holistic, in-depth approach undertaken, and its translation to inform practical, implementable risk management strategies. The research showed that the TP methods have the capacity to accommodate the reasons and activities responsible for adverse organisational outcomes, as well as the identification of the risks and their natures. A practice implication from the findings is that financial institutional risk should be managed in a holistic way, unencumbered by organisational boundaries that normally segment areas of work. This is because it was found that both the nature of risk, and the elements of the system of risk treatments, are all highly interconnected. This practical application utility is also
facilitated by taking a perspective that encompasses the entire organisation, in contrast to approaches that examine isolated activities or processes artificially removed from their organisational context.

1.9 Thesis structure

Chapter 1 of this thesis provides an introduction to the research. This chapter presents a brief description of the background of the research, the rationale for the research, the research aims and questions, and the research methodology used to meet the research objective.

Chapter 2 provides a review of the literature relevant to this research. First, supply chain risks are reviewed. This is followed by an examination of transactional risks. Next, the impacts of financial risks to both global and Australian financial institutions are discussed. Research on FSCR is then reviewed, and approaches to the management of risks in the supply chain are examined. Based on the literature, a conceptual model is presented that describes the major types of risk components of the supply chain, including demand and supply operations, information technology risk in the supply chain, and product management in the supply chain. Next, the complex multidetermined nature of risk is summarised, and TP methods used in applied risk operations research reviewed.

Chapter 3 describes the research methodology and the steps followed to meet the research aims, through the application of the adopted research strategy. First, the paradigm that forms the basis of the methods utilised to address the objective of this study is described. The methodology employed to address the research questions is explained, including how the cases were sampled and the participants selected. Finally, the structure and design of participant inquiries, the interviewing process and ethical considerations are described.
Chapter 4 describes the analysis and results of the current state analysis. It provides the findings of the application of the TP CRT method of inquiry with senior risk management participants from three financial institutions. First, it describes the nature of the function and structure of what the informant’s thought was typical of financial institutions in Australia. Second, it provides a description of the core risk effect types thought to face financial institution businesses. Third, the findings of the CRT method over three functional levels of financial institutions (the operations level, business strategy level and corporate strategy level) are presented, which describe the contributions to risk and the proposed causal pathways among the risk effects both at and between each functional level.

Chapter 5 describes the analysis and results of the desired future state analysis. It provides the findings of the application of the TP FRT method, which proposes a number of solutions that jointly respond to the risks identified from the CRT in Chapter 4. The FRT findings show what the participants considered a desirable future, where the risks previously identified are effectively controlled.

Chapter 6 provides a summary of how the research questions were answered, summarising the findings and describing how the research could be implemented in practice. Chapter 7 discusses the theoretical and practical contributions of the thesis and implications for future research. The limitations of the research are described, followed by a summary and conclusion of the research. Figure 1.1 illustrates the flow of chapters in this thesis.

### 1.10 Summary

In summary, this chapter provided a background to the importance of supply chain risk for financial institutions. Based on the literature, this chapter also identified research gaps regarding
the examination of FSCR and gaps relevant to Australian financial institution risk. The other major gap identified relates to taking a more holistic view of risk than was typically the case in previous research. The study’s research objective, developed in this chapter, is to create an in-depth understanding of risk and risk mitigation in Australian financial institutions. Finally, a brief discussion of the methodology used and the significance and limitations of the research were also presented in this chapter.
Figure 1.1 Overview of thesis structure

Chapter 1
Provides an introduction, background, research problems and questions, method outline, scope and contributions of the research

Chapter 2
Literature review about risk focusing on financial supply chain risk. A conceptual model is about risks components is developed. The Theory of Constraints operational risk mitigation approach is reviewed.

Chapter 3
Explains the research methodology and how the research questions are addressed. The multi-case study approach is described.

Chapter 4
Describes the analysis and results of the current state that illustrates the causal pathways amongst risk contributing organisational characteristics.

Chapter 5
Describes the analysis and results of a future state depicting a desired future where the organisational risks are effectively controlled.

Chapter 6
Comprises a discussion of the results and contextualises findings with the literature. Describes practical and research contributions, limitations and implications for future research.

Chapter 7
Provides the conclusion and summary of the research


CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter reviews the literature related to this research, especially the research related to financial risks from a supply chain perspective in the context of financial institutions, in three broad categories. First, identification of the range and diversity of supply chain risks is described. Second, the nature of organisational relationships with suppliers, customers, product management and technologies, particularly in the context of FSCR, is discussed. Third, FSCRM and risk mitigation are discussed.

This chapter is organised as follows. Section 2.2 discusses supply chain risks. Section 2.3 discusses the management of risks in the supply chain. Section 2.4 examines transactional risks. Section 2.5 discusses supply chain risk and Australian financial institutions. Section 2.6 examines FSCR. Section 2.7 reviews FSCR risk factor types. Section 2.8 describes the conceptual model of the major types of risk factors in the financial supply chain, including demand and supply, product management, and information technology risk in the supply chain. Section 2.9 describes FSCRM complexity accommodation and the TOC, which provides a holistic approach to the examination and explanation of organisational risk.

2.2 Supply chain risk

A supply chain perspective takes an inclusive ecological view of risk on organisational operations. This includes supplier and business-to-business processes through to customer end product delivery and includes business-to-customer processes such as the demand side of the supply chain
A supply chain view considers the entire organisational operating environment context, as well as discrete organisational characteristics. It refers to all business practices that are assimilated for the purpose of the provision of services and products required by consumers (Burgess, Singh & Koroglu 2006; Cousins et al. 2009; Harland 1996). While no agreed definition exists, authors have stressed the multifaceted and complex nature of supply chain risk (Fan & Stevenson 2018; Ho et al. 2015; Sohdi, Son & Tang 2012; Tang & Sodhi 2012). Ho et al. (2015) in a systematic review of the literature provided a comprehensive and inclusive definition (p. 5035) of supply chain risk: ‘the likelihood and impact of unexpected macro and/or micro level effects or conditions that adversely influence any part of a supply chain leading to operational, tactical, or strategic level failures or irregularities’.

Consistent with this definition, Ellram, Bals and Tate (2018) highlighted the importance of supply chain risks as significantly influencing competitiveness and organisational viability. Cavinato (2004) provided a useful conceptual overview of the characteristics of supply chains that have potential to contribute to risk. Cavinato (2004) proposed that supply chains consist of five inner-chain or network constructs: real, financial, educational, relational and innovative. The first, physical chains, represents traditionally viewed logistics, in the form of movement, storage, handling, processing, production and other forms of activities. Risks encompass transportation disruption, product loss, the inability to access inventories and supply discontinuity. Every supply chain also maintains a financial subchain working in parallel, in which parties in the chain have varying investments and costs, and cash movements and settlements from one firm to the next. These risks can arise through settlement process disruption, improper investments and by not bringing cost transparency to the overall supply chain (Cavinato 2004; Popa 2013). Security in settlement processes involving purchasing and distribution is an area of risk concern, as is the
management of securitised accounts receivables between firms (when this mechanism is in use) (Cavinato 2004; Ellram, Bals & Tate 2018; Shabbaz et al. 2018; Zhao & Huchzermeier 2015).

Informational subchains parallel the physical and financial chains through the processes and electronic systems used for creating effects and triggered product movements and service mobilisation. According to Cavinato (2004), a longer-term risk involves the creation and investment in information systems that are neither fully capable nor efficient for intended purposes and future business needs. Relational subchains relate to the chosen linkages among buyers, sellers and logistics partners. A spectrum of relationships that range from arm’s length price ones on the traditional side to closer and more sophisticated forms, which include cooperative, collaborative, innovation focused, joint venture and vertical integration forms of interorganisational relationships (Cavinato 2004; Ellram, Bals & Tate 2018).

Innovative subchains map the discovery, flow, creation and bring-to-market processes both within a firm and involving suppliers and other outsiders (Cavinato 2004; Sawik 2013). Supply here is the creation and bringing to market of a form of innovation for the benefit of the firm through increased market share or supply to new market segments. Innovative risk may represent the failure to effectively innovate and the loss of market share and reduced profitability.

Table 2.1 illustrates further supply chain risk definitions in the literature. The definition provided by Waters (2011) regarding any type of operational input as a potential source of risk is a more inclusive definition that comprises all supply chain inputs and their inherent risks. In contrast, the other definitions appear less inclusive; for example, Zsidisin and Ritchie (2009) focus on information and communication to the exclusion of other factors.
Table 2.1 Examples of supply chain risk definitions (compiled by author)

<table>
<thead>
<tr>
<th>Author</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ho et al. (2015)</td>
<td>The likelihood and impact of unexpected macro and/or micro level effects or conditions that adversely influence any part of a supply chain leading to operational, tactical or strategic level failures or irregularities</td>
</tr>
<tr>
<td>Jüttner, Peck &amp; Christopher (2003)</td>
<td>Any risks to the information, material and product flows from original suppliers to the delivery of the final product for the end user</td>
</tr>
<tr>
<td>Khan &amp; Zsidisin (2012)</td>
<td>Risk of any factor or effect that can materially disrupt a supply chain, whether within a single company or spread across multiple companies</td>
</tr>
<tr>
<td>Sodhi, Son &amp; Tang (2012)</td>
<td>Negative deviation from the expected value of a certain performance measure, resulting in negative consequences for the focal firm</td>
</tr>
<tr>
<td>Waters (2011)</td>
<td>Threat of risk to inward flows of any type of resource to enable operations to take place; also termed ‘input risk’</td>
</tr>
<tr>
<td>Zsidisin &amp; Ritchie (2009)</td>
<td>Threats and vulnerabilities of commercially acquired information and communications technologies within</td>
</tr>
</tbody>
</table>

Nixon et al (2003) defined service supply chain risk as a measure of the probability of a transaction failing. According to Wagner and Bode (2008, service supply chain risks are risks that are linked to the services, service provider or business and reduce the trust of services provided within the supply chain. Wagner and Bode (2011) argued that these risks are associated with transactions within the supply chain. For example, a customer may trust a supplier who is perceived as a high risk if the services offered by the supplier cost $12, but may not trust a high-risk supplier if the
supplied services cost $12,000. Table 2.2 illustrates other supply chain risk types that have been described in the literature.

There is a lack of consensus on which risks the supply chain may be exposed to, and many authors have attempted to create overarching classifications (Louis & Pagell 2019; Rangel, de Oliveira & Leite 2014). Perhaps in part reflecting the diversity and ecological complexity of the nature of multicomponent supply chains that also vary across industries, there is a large number of risk type classifications with diverse terminologies and definitions. Table 2.3 shows more recent supply chain risk classifications identified in the literature and illustrates both the diversity and complexity of risk classification, and where some authors have attempted, in turn, to re-classify the classifications (Louis & Pagell 2019; Rangel, de Oliveira & Leite 2014).

While there are a multitude of factors thought to contribute to risk of diminished performance (see Tables 2.2 and 2.3), part of the difficulty in creating a supply chain risk classification consensus may relate to the ambitious attempt to accommodate the diversity of all multi-industry factors associated with supply chains in general into a single descriptive classification. As the current research for this thesis has a focus on the financial supply chain in financial institutions, in particular, the remainder of this review narrows its focus to examining risks associated with the movement of financial products through transactions in the supply chain, through complex systems and processes to fulfil organisational purposes and objectives.
Table 2.2 Summary of supply chain risk types (compiled by author)

<table>
<thead>
<tr>
<th>Author</th>
<th>Risk Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cavinato (2004)</td>
<td>Physical, financial, informational, relational and innovative risks</td>
</tr>
<tr>
<td>Chopra &amp; Sodhi (2004)</td>
<td>Disruptions, delays, systems, forecast, intellectual property, procurement, receivables, inventory and capacity risks</td>
</tr>
<tr>
<td>Christopher &amp; Peck (2004)</td>
<td>External to the network, external to the firm but internal to the supply chain network: internal to the firm</td>
</tr>
<tr>
<td>Harland, Brenchley &amp; Walker (2003)</td>
<td>Strategic, operations, supply, customer, asset impairment, competitive, reputation, financial, fiscal, regulatory and legal risks</td>
</tr>
<tr>
<td>Jüttner, Peck &amp; Christopher (2003)</td>
<td>Environmental risk, network-related risk, organisational risk</td>
</tr>
<tr>
<td>Lin &amp; Zhou (2011)</td>
<td>Risk in the external environment</td>
</tr>
<tr>
<td>Louis &amp; Pagell (2019)</td>
<td>Internal to firm, internal to supply chain, external to supply chain</td>
</tr>
<tr>
<td>Manuj &amp; Mentzer (2008)</td>
<td>Supply, demand, operational and other risks</td>
</tr>
<tr>
<td>Ravindran et al. (2010)</td>
<td>Value at risk: labour strike, terrorist, natural disaster</td>
</tr>
<tr>
<td>Samvedi, Jain &amp; Chan (2013)</td>
<td>Supply, demand, process and environmental risks</td>
</tr>
<tr>
<td>Tang &amp; Musa (2011)</td>
<td>Material flow, financial flow and information flow risks</td>
</tr>
<tr>
<td>Tang &amp; Tomlin (2008)</td>
<td>Supply, process, demand, intellectual property, behavioural and political/social risks</td>
</tr>
<tr>
<td>Wagner &amp; Bode (2008)</td>
<td>Demand side, supply side, regulatory and legal, and infrastructure risk and catastrophic risks</td>
</tr>
</tbody>
</table>
Table 2.3 Examples of supply chain risk classifications (complied by author)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical</td>
<td>Environmental</td>
<td>Disruption</td>
<td>Demand</td>
<td>Strategic</td>
<td>Macro</td>
<td>Internal to firm</td>
<td>Internal to firm</td>
</tr>
<tr>
<td>Financial</td>
<td>Demand</td>
<td>Delays</td>
<td>Customer</td>
<td>Operations</td>
<td>Micro</td>
<td>Internal to firm</td>
<td>Internal to firm</td>
</tr>
<tr>
<td>Informational</td>
<td>Supply</td>
<td>Systems</td>
<td>Financial</td>
<td>Supply</td>
<td>(demand,</td>
<td>Internal to firm</td>
<td>Internal to firm</td>
</tr>
<tr>
<td>Relational</td>
<td>Control</td>
<td>Forecast</td>
<td>Weakness in</td>
<td>Customer</td>
<td>manufacturing,</td>
<td>Internal to firm</td>
<td>Internal to firm</td>
</tr>
<tr>
<td>Innovative</td>
<td>process</td>
<td>Intellectual</td>
<td>resources,</td>
<td>Asset</td>
<td>supply,</td>
<td>Internal to firm</td>
<td>Internal to firm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>property</td>
<td>development and</td>
<td>impairment</td>
<td>information,</td>
<td>Internal to firm</td>
<td>Internal to firm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Procurement</td>
<td>flexibility</td>
<td>Competitive</td>
<td>transportation,</td>
<td>Internal to firm</td>
<td>Internal to firm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Receivables</td>
<td></td>
<td>Reputational</td>
<td>financial</td>
<td>Internal to firm</td>
<td>Internal to firm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Inventory</td>
<td></td>
<td>Financial</td>
<td>Fiscal</td>
<td>External to firm</td>
<td>External to supply</td>
</tr>
<tr>
<td></td>
<td></td>
<td>capacity</td>
<td></td>
<td>plus</td>
<td>Regulatory</td>
<td>chain</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Legal</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interruption</td>
<td>Plan</td>
<td>Environmental</td>
<td>Value chain</td>
<td>Supply</td>
<td>Political</td>
<td>External controllable</td>
<td>External increase</td>
</tr>
<tr>
<td>Supply</td>
<td>Source</td>
<td>factors</td>
<td>Operational</td>
<td>Process</td>
<td>Economy</td>
<td>partially controllable</td>
<td>environment</td>
</tr>
<tr>
<td>Strategic</td>
<td>Making</td>
<td>organisational</td>
<td>Effect</td>
<td>Demand</td>
<td>Culture</td>
<td>External uncontrolled</td>
<td>Uncertainty between</td>
</tr>
<tr>
<td>Inertia</td>
<td>Delivery</td>
<td>factors</td>
<td>Credit</td>
<td>Intellectual</td>
<td>Technical</td>
<td>Internal controllable</td>
<td>node enterprises</td>
</tr>
<tr>
<td>Demand</td>
<td>Return</td>
<td>Industry factors</td>
<td>property</td>
<td>property</td>
<td>Natural</td>
<td>Internal uncontrolled</td>
<td>Uncertainly in</td>
</tr>
<tr>
<td>Capacity</td>
<td>Other</td>
<td>problems-specific factors</td>
<td>Behavioural</td>
<td>Behavioural</td>
<td>Demand</td>
<td>Internal partially controllable</td>
<td>node enterprises</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Decision maker</td>
<td>Political/Social</td>
<td></td>
<td>Logistics</td>
<td></td>
<td>Uncertainty in</td>
</tr>
<tr>
<td></td>
<td></td>
<td>factors</td>
<td></td>
<td></td>
<td>Capital</td>
<td></td>
<td>market demand</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2.3 Supply chain risk management

In the past, organisations have strategically used investments and other financial techniques to indirectly offset potential losses as an approach to manage financial risk (Ziman 2013). For instance, a number of studies of American companies show that over 60% employed derivative contract techniques (e.g., Wuttke, Blome & Henke 2013) to manage risk of future financial losses. Also, Viswanadham and Samvedi (2013) indicated that up to 90% of large firms in the UK use derivatives to manage risk of financial loss. Monitoring data from the Bank for International Settlements show increases in hedging investment (Sodhi, Son & Tang 2012). However, even with increased use of derivative contract techniques, the increase in financial risks has continued (Sodhi, Son & Tang 2012). In this section, rather than simply insuring against loss from uncontrolled risk (Wu, Blackhurst & Chidambaram 2006), more direct management of the supply chain risk within the potential control of an organisation is discussed.

Supply chain management is the management of all business practices that are assimilated for the purpose of the provision of services and products required by end consumers (Cousins et al. 2008; Harland 1996). Supply chain management also involves the strategic and systematic integration of tactics and traditional business practices across all business functions in the supply chain. This ultimately improves company performance in the long run as well as the supply chain as a whole (Mentzer et al. 2001).

Ho et al. (2015) noted that the majority of scholars have focused on manufacturing supply chains, whereas service supply chains have attracted less attention. In view of the importance of the role of service industries (Ho et al. 2015) and the fact that this research is concerned with supply chain risk in financial services, here, there is a focus on literature relating to services.
Supply managers navigate numerous hazards that exist in their increasingly competitive surroundings (Giunipero & Eltantawy 2004). Typically, this designed buffering is directed towards concerns of sub-optimal functional efficiency. Risk management may be a superior method to cope with these types of uncertainties by identifying possible cutbacks (Giunipero & Eltantawy 2004). According to Bambos (2011), service providers normally employ risk analysis methods to persuade their prospective service clients that their regular services are trustworthy. Moreover, environmental assumptions may be employed to characterise the assumptions of service providers regarding the infrastructure of prospective clients or partners in the supply chain (Govindan & Chaudhuri 2016).

Research by Belkhamza (2009) found that risk management may be adopted in a supply chain to secure cost-effective services that enable the development and application of cost-effective measures to decrease service supply chain risks. Service support and provision integrate or combine various technology control weaknesses and strengths for different parts of the supply chain, processes and technologies comprising a new service. At times, it may be beneficial to integrate risk management and technology assessments into service-related supply chains (Wan & Wan 2010). This process of integration is effective for the assessment of security weaknesses and strengths of the technology. Giunipero and Eltantawy (2012) proposed that service supply chain risk management processes provide details on who is accountable for performing the identified controls on a regular basis. This helps in maintaining services that are trustworthy to the potential partners or customers in a supply chain.

Fan and Stevenson (2018), in a review of SCRM, encapsulated the latter into four key stages: risk identification, assessment, treatment and monitoring. They concluded that much of the existing research tends to focus on single aspects of risk rather than taking a holistic approach, where all
four stages are examined together. They found that the monitoring stage, in particular, has received limited attention in the literature. While the risk of diminished performance can arise from any of the sources or stages of risk in the supply chain, the next section describes risk arising from transactional processes in the supply chain.

2.4 Transactional risks in the supply chain

Transaction processes are structured movements, economic incidents or exchanges that take place between two or more entities in a supply chain (Stair & Reynolds 2010). The transaction process system is a structured collection of devices, databases, procedures and people involved in the process of business transactions, and may be used to store data regarding the supply chain transactions (Stair & Reynolds 2010).

The transactional movements in the supply chain comprise a process component of the supply chain. Most companies aim to enhance their transactional activities, through such mechanisms as technology, costs and other variables, to reduce transaction time and costs, as well as for other benefits (Stair & Reynolds 2010). Supply chain transactions contain various transaction types, which serve effective and significant purposes in the business supply chain, such as ordering, commerce and socialising. A business may seek to enhance a supply chain transaction in which a single data or database source is inadequate in providing effective and reliable services to the customers and partners (Monczka & Handfield 2010).

According to Vrijhoef (2011), various market adjustment costs are greatly decreased or eliminated in well-managed supply chain transactions. For example, a business supply chain may use long-term contracts to reduce the total number of transactions and costs in a supply chain. In addition, the majority of consumers purchase most of their services and products through transactions
where the contractual basis is applicable to all the transactions and use of the transaction infers that an agreement has been established. Transaction process systems have been implemented by most companies or businesses with the main aim of storing, processing and collecting transactions and generating valuable documents associated with the management of business operations (Vrijhoef 2011).

Manual transaction processes require significant time input compared with computerised transactions to generate regular documents (Shah 2009). Moreover, computerised transaction processes and advancements in technology enable transaction supply chains to be operated or processed in a reliable and timely manner. These processes and arrangements enhance the activities in the supply chain. However, the advent in recent years of electronic transactions (Chaarani & Abaid 2018) has also introduced new risks, such as new types of fraud (Australian Payments Network 2018). Banks and other financial institutions are implementing various technologies and security systems to reduce or eliminate these types of financial supply chain transactional risks (Australian Payments Network 2018).

2.5 Supply chain risk and Australian financial institutions

In Australia, banks comprise both banking businesses as well as a range of other financial products such as insurance and investment products. For this reason, they are usually referred to as financial institutions in this thesis, but the term bank is also used where the literature refers to them as banking entities. There is a trend of increasing profitability of major banks (Reserve Bank of Australia 2018a), and Australian banks are among the most profitable in the world. According to 2015 data, the International Banker’s survey of the top 1000 banks around the world showed Australian banks make the highest profit as a share of GDP (cited in The Australia Institute 2018).
However, this profitability, according to the Reserve Bank of Australia (2017), partly reflects the more favourable economic conditions that prevailed in Australia in the period following the global financial crisis and a comparatively simple asset mix, with lower exposure to trading and institutional banking. Also contributing to higher profitability is that Australian net interest margins are higher than in a number of other countries (Reserve Bank of Australia 2017).

Despite increased profitability, most banks, both globally and domestically, are vulnerable to risk factors. For example, financial institution risk has received considerable public attention in the Australian media. The terms of reference of the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry (Royal Commission) in 2017 (Commonwealth of Australia 2018, p. 2) aimed to examine:

- ‘The adequacy of the existing laws and policies of the Commonwealth relating to the provision of banking and related financial services;
- The adequacy of the internal systems of financial services entities;
- The adequacy of existing forms of industry self-regulation, including industry codes of conduct, to identify, regulate and address misconduct and conduct falling short of community expectations and to provide appropriate redress to consumers;
- The effectiveness and ability of regulators to identify and address misconduct;
- Whether any further changes to the legal framework, practices within entities, or the financial regulators are necessary to minimise the likelihood of misconduct in the future; and
- The effectiveness of mechanisms for redress for consumers of financial services who suffer detriment as a result of misconduct.’
Risks that affect institutional performance also include loss of public confidence, risk of reputation loss and customer dissatisfaction, where customers convert to sector competitors. Banking and other financial institution misconduct is noted in the interim report’s executive summary (p. 1), which found that ‘conduct by financial services entities that has brought public attention and condemnation’, and that the major financial institutions all acknowledged misconduct (Commonwealth of Australia 2018).

The Royal Commission (Commonwealth of Australia 2019) found deficiencies of culture, governance and risk management within Australian banks. The deficiencies found in Australian banking practices reflected scandals and prudential concerns about effective governance, risk management, risk controls and incentive-based compensation that had also occurred in Europe and North America. This deficiency in risk management affects the banks’ prudential standing and was thought to significantly reduce the value of their issued capital. The report found that the conduct by financial services entities had brought public attention and condemnation, and that the major financial institutions all acknowledged misconduct. The disclosures in public hearings prompted banks and regulatory authorities to begin to consider how to address shortcomings in risk management and misconduct (Commonwealth of Australia 2019).

Financial transaction risks in banking supply chains are also vulnerable to risk, including theft and unlawful bank transactions (Association of Financial Professionals 2017; Australian Payments Network 2018). According to a survey carried out by the Association of Financial Professionals (2014), 90% of respondents indicated that risk management was strategically important and 84% of respondents indicated that their organisations had increased exposure to risk relative to the previous three years.
This increased risk perception coincides with the increasing automation and electronification of financial transactions (Chaarani & Abiad 2018), such as contactless card payments (Australian Payments Network 2018). These changes may have implications for the nature of the risks and the potential for financial loss and present new challenges for contemporary banking organisations. Financial institutions, in particular, face major risks, including fraud, because of the movement of financial products from one point to another (ACI Worldwide 2016; Australian Payments Network 2018).

Technology-related impacts of FSCR occur when technology services provider failures cause major disruptions, such as when network services cause national outages and mean that bank customers are unable to use payment cards or ATMs, leading to nationwide retail and other business disruptions. For example, the Australian provider of banking network services caused a national outage that left many bank customers across Australia unable to use EFTPOS or ATMs, leading to nationwide retail and other business disruptions (Withers 2018).

The literature regarding impact of risk on Australian financial institutions illustrates the importance of understanding the contribution of supply chain risk. The supply chain is an essential part of business operations (Fan & Stevenson 2018), and this is particularly so for financial institutions where the product is usually comprised of some aspect of money and the delivery of financial services, which involves the movement of money through a network of financial transaction processes. The financial supply chain, discussed in the next section, is an important part of supply chain transactions, management and business operations.
2.6 Financial supply chain risk

Ho et al.’s (2015) definition of supply chain risk described in Section 2.2 is adapted for this research on financial-related risks from a supply chain perspective. The definition in this research of FSCR is the likelihood and impact of unexpected macro- and/or micro-level financial-related effects or conditions that adversely influence any aspect of a supply chain and can lead to operational, tactical or strategic level failures or irregularities. This definition encompasses supply chain financing risk related to risk concerning adequate funding of supply chain activity (Popa 2013). It is also more inclusive than the finance perspective described by Fan and Stevenson (2018) related to accounting, such as working capital optimisation, asset financing, and so on. Table 2.4 lists several definitions of FSCR that have appeared in the literature.

Importantly, the supply chain in financial institutions is unlike the physical products or non-financial-related service products of non-financial service businesses. In the latter, the financial and non-financial aspects of supply chain risk are sometimes definitionally separated (Popa 2013). However, banking and financial institutions deal almost exclusively with products and services that are essentially financial in character. Therefore, the financial and non-financial aspects of financial institutions’ supply chain risk do not appear to be so easily separated. For example, the functional banking equivalent of the logistics of the movement of goods through a supply chain is the movement of money through electronic banking networks. Further, it is possible that financial-related risks may interact with financial risks and that their potential joint effects may not be easily separated or attributed. In this research, a more inclusive definition of FSCR is adopted to accommodate the financial nature of the institutions under investigation.

The financial attributes of the supply chain have been described as including a set or series of financial operations for the safe transportation, distribution and storage of products or services
Table 2.4 Definitions of FSCR (compiled by author)

<table>
<thead>
<tr>
<th>Author</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Belkhamza (2009)</td>
<td>Chance that business cash flows are not sufficient to pay creditors and fulfil other financial responsibilities</td>
</tr>
<tr>
<td>Cousins &amp; Lawson (2007)</td>
<td>Variability of actual returns on an investment around an expected return, even when those returns represent positive outcomes</td>
</tr>
<tr>
<td>Hull (2012)</td>
<td>Risk that involves financial loss to firms; financial risk because of instability and losses in the financial market caused by factors such as movements in stock prices, currencies and interest rates</td>
</tr>
<tr>
<td>Gelsomino et al. (2016)</td>
<td>Short-term risk accounts payable risk and supply chain finance risk related to lack of working capital optimisation</td>
</tr>
<tr>
<td>Manuj &amp; Mentzer (2008)</td>
<td>Risk that a firm will be unable to meet its financial obligations; risk is primarily a function of the relative amount of debt that the firm uses to finance its assets</td>
</tr>
<tr>
<td>Popa (2013)</td>
<td>Risk from activities of planning and controlling all financial processes, within a company and for communication with other enterprises</td>
</tr>
<tr>
<td>Stair &amp; Reynolds (2010)</td>
<td>Possibility that a bond issuer will default by failing to repay principal and interest in a timely manner</td>
</tr>
<tr>
<td>Wan &amp; Wan (2010)</td>
<td>Probability of loss inherent in financing methods that may impair the ability to provide an adequate return</td>
</tr>
<tr>
<td>Yeates (2014)</td>
<td>Risk that an effect will trigger a loss of economic value or confidence in a substantial portion of the financial system, and increases in uncertainty about the financial system that is serious enough to have significant adverse effects.</td>
</tr>
</tbody>
</table>

within a network of industries (Vanany & Pujawan 2009). In financial institutions, particularly, products can include money as well as efficient cash flow and working capital availability.  

According to Berger and Humphrey (1997), efficient supply chain management has continuously reported viable and successful business flows in various markets. With increasingly fierce
competition in the business world, FSC risk management has become a point of focus for companies across the globe. In a large survey of 760 German managers, Wagner and Bode (2006) suggested that multiple components of a supply chain, including those that are financial in nature, contribute risk to all industries. Reducing risk in the FSC creates a competitive advantage over other financial institutions in similar markets (Berger & Humphrey 1997). Increases in disasters and catastrophes have intensified the need for firms and industries to search for ways of combating supply chain vulnerability and risks (Bode et al. 2011; Wagner & Bode 2008). As the costs of the capital resources of the supply chain continue to increase, the process of managing capital and cash flows becomes as essential as managing interactions between supply chain partners (Blome & Schoenherr 2011). With only two studies found, there is limited research on supply chain risk in financial institutions (Blome & Schoenherr 2011; Lundin 2012); further, no studies could be found about FSCR in Australian financial institutions.

2.6.1 Financial supply chain risk management

Following a comprehensive review of supply chain risk management, Fan and Stevenson (2018, p. 210) defined this as:

The identification, assessment, treatment, and monitoring of supply chain risks, with the aid of the internal implementation of tools, techniques and strategies and of external coordination and collaboration with supply chain members so as to reduce vulnerability and ensure continuity coupled with profitability, leading to competitive advantage.

Table 2.5 shows contributions regarding FSCR management. These FSCR management strategies and techniques address the exceptional risks encountered along the supply chain by implementing
continuous risk evaluation and assessment to minimise vulnerability and exposure to ensure the continuity of effective product supply. The risk mitigation strategies include both financial and operational management strategies (Bandaly et al. 2013; Murali & Rajkumar 2018; Takeishi 2001).

Table 2.5 Contributions regarding FSCR management (compiled by author)

<table>
<thead>
<tr>
<th>Author</th>
<th>Area of Interest</th>
<th>Contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandaly et al. (2013)</td>
<td>Supply chain management</td>
<td>Impact of risk-averse strategy in supply chain</td>
</tr>
<tr>
<td>Blome &amp; Schoenherr (2011)</td>
<td>Supply chain risk management</td>
<td>How companies manage financial crises within the supply chain</td>
</tr>
<tr>
<td>Ceryno et al. (2013)</td>
<td>Supply chain risk management</td>
<td>Concepts and strategies within supply chain risk management</td>
</tr>
<tr>
<td>Christopher &amp; Lee (2004)</td>
<td>Supply chain risk</td>
<td>Enhancing confidence to reduce supply chain risks</td>
</tr>
<tr>
<td>Fan &amp; Stevenson (2018)</td>
<td>Supply chain risk management</td>
<td>Review of SCRM, definitions and theory with research agenda recommendations</td>
</tr>
<tr>
<td>Olson &amp; Wu (2010)</td>
<td>Risk management</td>
<td>Generic risk supply chain framework</td>
</tr>
<tr>
<td>Zhao &amp; Huchzermeier (2015)</td>
<td>Risk management</td>
<td>Framework to integrate analytical operations–finance interface models</td>
</tr>
<tr>
<td>Wagner &amp; Bode (2008)</td>
<td>Supply chain performance</td>
<td>Measures and strategies to mitigate FSCRs</td>
</tr>
</tbody>
</table>
FSCR were considered by Blome and Scheonherr (2011) to be one of the more significant contributors to performance risk, and able to serve as barriers to risk remediation. In response to FSCR, some industries have combined their efforts to ensure effective and efficient demand, supply and financial and transportation management (Wagner & Bode 2008). Supply chain financial risk management is primarily aimed at managing the risks in complex dynamic supply and demand networks (Dyer & Singh 1998; Dyer Singh & Hesterly 2018). FSCR management considers the key strategy for managing the exceptional risks that are encountered along the supply chain processes.

A common theme in the literature is that managing risk is based on continuous risk evaluation and assessment with the purpose of minimising vulnerability and exposure to ensure continuity of effective product supply in the chain. This is supported by Fan and Stevenson (2018), who, in their review of supply chain risk management, followed the typology of Hallikas et al. (2004) and distilled the literature into four key processes: risk identification, assessment, treatment and monitoring. Although Zsidisin and Ritchie (2009) added a fifth step, organisational and personal learning, in this research, Fan and Stevenson’s definition is adapted to FSCR management and is here defined as the identification, assessment, treatment and monitoring of financial supply chain risks, with the aid of the internal implementation of tools, techniques and strategies and of external coordination and collaboration with supply chain members to reduce vulnerability and ensure continuity coupled with profitability, leading to competitive advantage.

### 2.7 Financial supply chain risk factors

The literature on the exposure of the supply chain to different types of risk is examined in the following sections to identify potential factors that could cause disruption in the financial supply chain where those risks could be relevant to financial services. The following sections describing
FSCR types are adapted, organised and based on risk factor categories from the supply chain risk factor categories distilled by Tang (2006) and Ho et al. (2015) in their literature reviews on supply chain risks. These categorisations of risks are demand risk factors, supply risk factors, product management risk factors and information management risk factors.

### 2.7.1 Demand risk factors

Demand refers to processes related to business-to-customer interfaces, including retailer relationships and outbound processes (Tang 2006; Ho et al. 2015; Zhao & Huchzermeier 2015). In every market, there is demand for money from both buyers and sellers. Operational demand management (ODM) refers to establishing profitability by meeting customer demands and expectations while ensuring delivery of high-quality service (Christopher 2016). At the strategic stage, the organisation efficiently handles the total demand as it acquires new technology, skills and infrastructure. At the tactical stage, the organisation aligns resources to enhance value to the customer in a profitable way. ODM mandates the provision of reliable delivery tasks that occur within the constraints of the supply chain (Christopher 2016).

There are risks associated with demand creation, supply planning, order management and communication. In a review of the literature, Ho et al. (2015) examined a number of demand-related risks. Table 2.6 shows a summary list of demand risk factors that have been identified in the supply chain. Demand risks are further discussed and synthesised by Cousins et al. (2008) into three types related to shifting demand over time, shifting demand across markets, and demand shift against products.
Table 2.6 Summary list of demand risk factors in the supply chain (compiled by author)

<table>
<thead>
<tr>
<th>Demand risk factors</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inaccurate demand forecasts (Chopra &amp; Sodhi 2004)</td>
<td></td>
</tr>
<tr>
<td>Serious forecasting errors (Manuj &amp; Mentzer 2008)</td>
<td></td>
</tr>
<tr>
<td>Unmanaged demand variability or information distortion (Tummala &amp; Schoenherr 2011)</td>
<td></td>
</tr>
<tr>
<td>Demand uncertainty (Hahn &amp; Kuhn 2012)</td>
<td></td>
</tr>
<tr>
<td>Sudden shoot-up demand (Samvedi, Jain &amp; Chan 2013)</td>
<td></td>
</tr>
<tr>
<td>Demand variability (Chopra &amp; Sodhi 2004)</td>
<td></td>
</tr>
<tr>
<td>Customer fragmentation (Gaudenzi &amp; Borghesi 2006)</td>
<td></td>
</tr>
<tr>
<td>High level of service required by customers (Gaudenzi &amp; Borghesi 2006)</td>
<td></td>
</tr>
<tr>
<td>Customer dependency (Wagner &amp; Neshat 2010)</td>
<td></td>
</tr>
<tr>
<td>Deficient or missing customer relation management function (Tuncel &amp; Alpan 2010)</td>
<td></td>
</tr>
</tbody>
</table>

2.7.1.1 Shifting demand across time

In demand management, shifting demand across time is considered essential (Cousins et al. 2008). It has been argued that the following factors should be considered when shifting demand. During high or peak seasons, service industries should increase prices (Cousins et al. 2008). During low-demand seasons, discount strategies should be implemented, advance purchase of goods should be encouraged and various payment methods should be incorporated with strategies for postponing demand, such as offering price discounts to clients who accept late shipments (Cousins et al. 2008).

2.7.1.2 Shifting demand across markets

To manage demand against the market, it has been suggested that industries should ensure that when they are selling products that have short life cycles, product rollovers should be properly managed (Cousins et al. 2008). Further, Cousins et al. (2008) proposed that to mitigate risk,
industries might consider selling new products and commodities in different markets, shifting demand from the primary market to a secondary market or implementing trans-shipments.

2.7.1.3 Demand shift against products

To ensure an optimum balance of shifting demand against products, an industry should ensure that it is selling multiple products and commodities in a single market, and that promotion and pricing strategies entice clients to switch to different brands or products (Cousins et al. 2008).

The ultimate purpose of marketing strategies is to assist firms in increasing market share, revenue and sales (Cousins et al. 2008). Product substitution can be achieved through selling products containing similar features to improve a firm’s product substitutability (McGinnis & Vallopra 1999). Product substitution occurs when a product dominates the other products in performance or quality (McGinnis & Vallopra 1999). Product bundling helps a firm to change the demand for its commodities and products by structuring bundles (Handfield & Bechtel 2002). Examples can be identified across a wide range of products, including food, apparel, cosmetics and electronics. When a product or commodity is sold in bundles, customers are forced to buy all of the commodities and products as a bundle. This, in turn, increases demand for the products (Handfield & Bechtel 2002).

This examination of the literature shows that a number of risks have been identified in the literature associated with demand operations that govern outbound transactions, usually in the business-to-retail-customer interface of the supply chain. More recently, Shahbaz et al. (2018) proposed a conceptual model that incorporates several risk source categories, including generic demand-side risks, as well as supply-side risks. Next, supply risks are discussed.
2.7.2 Supply risk factors

Supply operations risk is a broad term used to describe various ways of acquiring, managing and identifying the products and resources necessary to manage a business or any organisation successfully and effectively (Cousins et al. 2008). Supply management components are tools with fundamental significance in financial supply chain management (Clark & Fujimoto 1991). They assist in the management of the resources and products that are associated with the capabilities that an organisation or industry requires to explore its maximum potential to meet or attain its targeted objectives (Cousins et al. 2008). In a review of the literature, Ho et al. (2015) described a number of supply chain related risk factors (see Table 2.7). Supply operations management ensures the effective flow of resources and products to meet client demand. To demonstrate effective supply, there should be both physical and information flows (Handfield 2013).

Physical supply comprises the movement of goods within the market (transportation), whereas information supply is effective communication within the chain. For effective and efficient supply network design, an industry must ensure good network configuration, product and transportation planning, and product and customer assignment (Liker et al. 1996). Table 2.8 shows examples of supply operations risks.

2.7.2.1 Supply network design

For effective and efficient supply network design, an industry should ensure that there is good network configuration, product planning, transportation planning, product assignment and customer assignment (Liker et al. 1996). Network configuration ensures that there is effective communication to ensure that goods have been supplied appropriately (Liker et al. 1996). Liker et al. (1996) also argued that transportation of the product should be planned and that the product to be transported must be well packed. If products are fragile or perishable, the most suitable
method of transportation should be selected to ensure that the supply is completed without problems (Liker et al. 1996).

Table 2.7 Summary list of supply risk factors in the supply chain (compiled by author)

<table>
<thead>
<tr>
<th>Authors</th>
<th>Supply risk factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zsidisin &amp; Ellram (2003)</td>
<td>• Inability to handle volume demand changes</td>
</tr>
<tr>
<td></td>
<td>• Failures to make delivery requirements</td>
</tr>
<tr>
<td></td>
<td>• Cannot provide competitive pricing</td>
</tr>
<tr>
<td></td>
<td>• Technologically behind competitors</td>
</tr>
<tr>
<td></td>
<td>• Inability to meet quality requirements</td>
</tr>
<tr>
<td>Chopra &amp; Sodhi (2004)</td>
<td>• Supplier bankruptcy</td>
</tr>
<tr>
<td></td>
<td>• Single supply sourcing</td>
</tr>
<tr>
<td></td>
<td>• Small supply base</td>
</tr>
<tr>
<td></td>
<td>• Supplier dependency</td>
</tr>
<tr>
<td></td>
<td>• Global outsourcing</td>
</tr>
<tr>
<td>Tummala &amp; Schoenherr (2011)</td>
<td>• Supply responsiveness</td>
</tr>
<tr>
<td></td>
<td>• High capacity utilisation at supply source</td>
</tr>
<tr>
<td>Gaudenzi &amp; Borgesi (2006)</td>
<td>• Narrow number of intermediate suppliers</td>
</tr>
<tr>
<td></td>
<td>• Lack of integration with suppliers</td>
</tr>
<tr>
<td></td>
<td>• Lack of supplier visibility</td>
</tr>
</tbody>
</table>

2.7.2.2 Supplier relationships

According to Handfield et al (2013), supplier relationships are a source of risk. The interorganisational relationship between a company and supplier is crucial to the supply chain,
where it can be beneficially cooperative rather than adversarial (LaBahn & Krapfel 2000; Leuschner, Rogers & Charvet 2013; Primo & Amundson 2002). In addition, in organisations that operate internationally, cross-cultural relationship building is needed to create a mutually beneficial financial partnership. Cultural adaption is the strategy that has been put forward as a prime mitigation strategy for addressing cultural diversity related risks (Monczka et al. 1998). This could include intercultural sensitivity and cultural awareness enhancement approaches (Progoulaki & Theotokas 2016).

Table 2.8 Supply risk examples (compiled by author)

<table>
<thead>
<tr>
<th>Author</th>
<th>Area of Interest</th>
<th>Contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clark &amp; Fujimoto (1991)</td>
<td>Supply network design</td>
<td>Effect of management, organisation and strategy on this critical constituent of business strategy</td>
</tr>
<tr>
<td>Handfield et al (2013)</td>
<td>Financial risk</td>
<td>Strategies to reduce disruptions in the supply chain</td>
</tr>
<tr>
<td>Liker et al. (1996)</td>
<td>Supply involvement</td>
<td>Mutual dependence, competition, performance monitoring and target prices to control suppliers</td>
</tr>
<tr>
<td>Wagner &amp; Bode (2008)</td>
<td>Supplier relationships</td>
<td>Factors (external and internal) that affect supply chain risk exposure</td>
</tr>
<tr>
<td>Womack, Jones &amp; Roos (1991)</td>
<td>Lean production</td>
<td>Transformation of traditional enterprises into paradigms of lean success</td>
</tr>
</tbody>
</table>

In relation to financial risks, Handfield et al (2013) suggested that various types of supplier relationships, ranging from a single-time purchase to virtual integration, should be considered for adoption. Four types of relationships exist in supply chain management to ensure successful
delivery and distribution of goods among clients or consumers (Handfield et al 2013): vendor, exclusive supplier, partner and preferred supplier. In addition, Handfield et al (2013) suggest that long-term and short-term contract issues should be transparently explored and elaborated to ensure that there is a proper supply of goods in the market.

2.7.2.3 Supplier order allocation

Supplier order allocation addresses uncertain demand, uncertain supply, uncertain supply lead-time and uncertain price of products (Handfield et al. 1999; Handfield et al. 2009). Uncertain price or cost relates to the currency rates that are set in the international market. It also includes the upstream cost that is implemented by partners, as well as the flexibility of changing between two plants located in different nations (Handfield et al. 1999; Handfield et al. 2009). Uncertain supply lead-time occurs when replenish lead-time determines demand. Uncertain supply denotes cases where buyers receive random orders. Uncertain demand entails allocation of single suppliers and restriction to two suppliers because of complexity (Handfield et al. 1999; Handfield et al. 2009; Leuschner, Rogers & Charvet 2013).

2.7.2.4 Supply contracts

Supply partners in various organisations and industries make numerous independent decisions that differ from each other. Locally, decisions are always operationally inefficient or globally sub-optimal, causing an inadequate or malfunctioning supply chain. According to Wagner and Bode (2006), a disintegrated or fragmented supply chain occurs because of customer demand, because individuals attempt or seek to maximise their personal interest. Optimal decisions that are made locally can culminate in complete disruption of the supply chain (Siddiqi 2017; Wagner & Bode 2006).
2.7.3 Information systems management risk factors

The application of information technology (IT) can enhance supply chain management and contribute to competitive advantage. IT can deliver competitive positioning of business resourcefulness, such as restructured cross-functional processes and reduced cycle time (e.g., Tang & Musa 2011). IT inventions generate different techniques for organisations to manage supply chain interactions. IT enables the easy flow of information, materials and finance among customers, manufacturers, distributors and suppliers (Olsen & Wu 2010). Therefore, IT is a major tool for minimising supply chain risks effectively and efficiently. For example, a bank can use different analytic methods to explore the potential effects of currency exchange rates and changes in supply chain prices to reduce the risks involved.

Prior to the application of computers and technology, information flow among the various functions and departments of a firm and other related firms in the supply chain was paper based. This meant that the dissemination of information was a slow process, vulnerable to complete distortion. There were many irregularities in the supply chain that might have led to customer dissatisfaction. However, the application of IT has eased processes and communication in the supply chain (Cavinato 2004).

Companies are becoming increasingly aware of the need to depend on efficient supply chain networks to enhance their competitive advantage in the market, as well as reduce financial risks involved in marketplaces. Customer uptake of mobile and online banking services is increasingly important service provision and depends on perceived usefulness, among several other factors including trust (Jalil, Talukder & Rahman 2014; Martins, Oliveira & Popovič 2014; Talukder, Quazi & Sathye 2014) and managerial reforms (Saneie & Naghneh 2015). In the past few years, IT, outsourcing and supply chain globalisation have allowed most companies to effectively reduce
financial risks and enhance collaboration among partners within supply chain networks. Risks can be reduced when every specialised business partner in the supply chain concentrates on a few strategic activities, or even a sole activity (English et al. 2003; Ho et al. 2012; Primo & Amundson 2002).

Chen, Paulraj and Lado (2004) suggested that strategic purchasing, top management support and establishing competitive priorities affect the efficient management of the supply chain. Considering that an organisation depends on interorganisational relationships for the supply chain to operate, the use of IT can assist building these relationships to reduce risk (Primo & Amundson 2002).

Supply network structure is a construct that addresses a non-power, horizontal and decentralised structural link between different participants of the supply chain (Harland, Brenchley & Walker 2003). In this construct framework, logistics integration assesses the extent of materials and information integration across the supply chain to determine where information could improve performance.

Uncertainty is another fundamental construct in general business management, such as strategic management, marketing and organisational theory. There are three key uncertainty sources that influence a company’s supply chain: demand and customer uncertainty, originating from irregular orders and prediction of errors; manufacturing uncertainty, originating from supply chain performance, machine failure and process performance; and supplier uncertainty, originating from the degree of discrepancy, average lateness and on-time performance (Flynn, Koufteros & Lu 2016). Flynn, Koufteros and Lu (2016) also suggested that increased competition in global and local markets and the increase in technology-related innovation are the main fundamental factors compelling business needs for first-class suppliers and for advancement of suppliers.
The use of IT adds a competitive advantage to businesses seeking to manage FSCR (Nair, Raju & Anbudayashankar 2009). According to Nair, Raju and Anbudayashankar (2009), these tools facilitate the competitive positioning of business resources by restructuring cross-functional processes and reducing cycle time. IT inventions are constantly generating innovative techniques whereby organisations can more effectively manage supply chain interactions. The tools enable the easy flow of information, materials and finances among customers, manufacturers, distributors and suppliers, making IT one of the most significant contributors to successful supply chain management (e.g., Dyer & Hatch 2004; Schlegel & Trent 2014; Pfohl, Köhler & Thomas 2010).

2.7.3.1 Information accuracy and sharing

Sharing accurate information about supply and demand of the supply chain can result in performance improvements for all individuals in the supply chain (Dyer & Hatch 2004). Accurate information supply can be achieved through adaption of advanced technologies, which can make communication faster. Jappelli and Pagano (2002 presented evidence of both the benefits of modern trends in interorganisational information sharing as well as regulatory risks to protect consumer rights. Both Adeosun et al. (2008) and Bloom et al. (2014) described various benefits and risks associated with modern IT’s effects on communications and information sharing. Agboola (2007) argued that competition is a driving force for the greater uptake of IT.

2.7.3.2 Information system security and disruption

Information system security entails safeguarding vital information from unauthorised access, disruption and investigation. Exposure of a firm’s vital information may lead to supply chain risk (Schlegel & Trent 2014). The most effective way to manage this issue is to use electronic computers to safeguard information. Passwords can be set to preffect bypass (Pfohl, Köhler & Thomas 2010). Barth et al. (2009) suggested that information sharing can reduce corruption.
DuHadway and Carnovale (2019) examined the role of relational risk associated with other companies or individuals in the supply chain engaging in malicious behaviours that can lead to disruptions. They suggested that effective detection, which comes from information sharing, new technologies, supply chain visibility and supplier integration, can detect or prevent a variety of disruptions, together with other benefits from supplier integration into the supply chain (Petersen, Handfield & Ragatz 2005).

The advent in recent years of electronic transactions (Chaarani & Abaid 2018) has also introduced new risks, such as new types of fraud (Australian Payments Network 2018). As a result of increasing ATM and debit and credit card fraud and theft, banks and other financial institutions implement various technologies and security systems to reduce or eliminate these types of bank fraud. Even though the occurrences of credit card fraud represent only 0.2% of all credit card transactions, this results in extensive financial losses (Australian Payments Network 2018). For example, of 8.9 billion card transactions in Australia in 2017, $561 million in value was lost to card-related fraud (Australian Payments Network 2018). Although there are some refined fraud prevention and detection systems adopted by all banks, such as card chip technology, bank fraud remains a critical focus, particularly in information systems related card-not-present fraud typical of internet-based financial transactions. Likewise, bank fraud has affected many banks across the globe. For example, according to ACI Worldwide (2016), 30% of consumers globally have experienced payment card fraud in the past five years.

Additionally, offenders target ATMs, installing ‘skimmers’ near the locations in which bank customers insert their cards; card details are copied and later used for fraudulent transactions. To further illustrate the extent of financial transaction risks, in Australia, there was an estimated one
ATM fraud per 1.1 million transactions in 2012, with a loss of A$23 million in 2016 (Australian Payments Network 2016).

Table 2.9 shows that Deutsche Bank, Bank of Africa and NAB are among the banks that experienced the greatest all-cause losses reported in 2014 (Australian Payments Clearing Association 2014). The main factors for these losses were management and global financial instability, but fraud was also a factor, primarily skimming and counterfeit cards (DuHadway & Carnovale 2019; Yeates 2014).

According to Yeates (2014), in Australia, approximately 3.4% of losses were the result of fraud. The total fraud on cheques and cards increased from 16 cents per A$1000 in 2012 to 17 cents per A$1000 in 2013. The total number of fraud incidents on payment cards rose by 15%, accounting for A$304 million and an increase of 5% to A$634 billion on the entire sum of money spent in Australia using cards (Yeates 2014). Moreover, there was an increase from 15 cents to 17 cents in every A$1000 transacted on cheque fraud, where the entire fraud on cheque payments increased by 13% to A$7 million, in contrast to an increase of 1.3% to A$1330 billion in the entire sum of money transacted on cheques (Yeates 2014).

Although there was a decrease in skimming and counterfeit fraud on all cards by 47% from 2008 to 2017 (Australian Payments Network 2018), the cost of skimming fraud is still substantial. The amount of loss was A$11 million in 2013. The highest skimming fraud on cards in Australia was experienced in 2008, followed by 2011, with a decreasing trend for 2017. The difference between Australia and overseas is attributed to the greater utilisation of card chip technology in Australia (Australian Payments Network 2018).
Table 2.9 Banks with the greatest all-cause losses (adapted from Australian Payments Clearing Association 2014)

<table>
<thead>
<tr>
<th>Bank</th>
<th>Country</th>
<th>Loss (A$ Billion)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deutsche Bank</td>
<td>United Kingdom</td>
<td>1.30</td>
</tr>
<tr>
<td>Bank of Africa</td>
<td>United States</td>
<td>0.45</td>
</tr>
<tr>
<td>National Australia Bank</td>
<td>Australia</td>
<td>0.36</td>
</tr>
</tbody>
</table>

2.7.3.3 Information availability and outsourcing

Information about a firm’s products should be available to individuals in the industry to eliminate risk in the supply chain. Information about the cost or price of commodities should be communicated (Dyer 1996). Introduction of new products in the market should also be communicated (Dyer & Hatch 2004). This can be achieved through IT implemented in firms, which assists in cutting costs and minimising risks (Dyer & Hatch 2004). Further, information availability has many contributions to make in minimising risk in the supply chain (DuHadway & Carnovale 2019; Kallberg & Udell 2003) as well as outsourcing information supply to external information providers (Barth et al. 2009; Dong, Xu & Zhu 2009; Wallenburg et al. 2011).

2.7.3.4 Communication and technology

Communication is a vital component of supply chain management. It holds fundamental significance in the process of minimising risks of a supply chain (Primo & Amundson 2002; Bloom et al. 2014), and is a crucial factor behind the success and prosperity of numerous firms, linking the firm to clients. Communication can be made effective via the implementation of good sales persons, as well as by implementation of effective communication technologies.
Adopting supply chain strategies and operations enhances efficiency and effectiveness of supply chain processes and promotes extensive innovation along the value chain (Schlegel & Trent 2014). Attaining effective data integration in the supply chain is thought to require effective data quality management (Giunipero & Eltantawy 2004).

2.7.4 Product management risk factors

When operating in competitive environments, businesses can adopt a strategy to expand or diversify products to maintain and increase competitiveness (Handfield & Bechtel 2002). This has been particularly important for financial institutions following the global financial crisis. A variety of products allows financial institutions to increase market share and revenues (Hull 2012).

2.7.4.1 Product lifecycle

When a product is introduced in the market, suppliers should ensure that sales volume and product supply are low to ensure that no loss is encountered. As product demand gradually increases, sales volume should also increase. Then, as the product reaches maturity, supply should be high and correspond to demand. The sales volume of the product declines when a new product is introduced, providing an alternative to the initial product (Mohr & Spekman 1994). According to Albers, Wohlgezogen and Zajac (2016), strategic alliances among partners in the supply chain can reduce product management risk and enhance competitiveness.

2.7.4.2 Delivery time

As demand increases, delivery time may be delayed. An industry or firm should incorporate strategies that will assist in meeting the needs of clients (Clark 1989; Miemczyk & Holweg 2004); for example, offering discounts to clients who accept late or extended deliveries (Marsh & Stock 2003). Myrelid and Jonsson (2018) argued that the delivery time of information is a determinant of relational quality among collaborators in the supply chain.
2.7.4.3 Political management

Emerging markets and industries have continuously grown and become attractive to businesses seeking alternative areas and sectors for growth. Supply chains with less mature economic contracts, loans and assets may suffer severe adverse impacts from government actions (Dyer 1996). Supply chains have become increasingly exposed and vulnerable to governments and political leaders who are exploiting the field. According to political risk indicator maps (Wu & Blackhurst 2009), risk has been noted to increase with political activities that disrupt the supply chain, such as government strikes, embargoes, riots, interference and civil commotion (Hull 2012; Smith 2019).

2.7.4.4 Political risk tracker

The political risk tracker (Ragatz, Handfield & Petersen 2002) helps in assessing the impact of politics on supply chain management. It provides 10-year historic prices and the current transaction price, entailing capacity and rating data including 100 countries. The tracker also assists with providing a transparent project future for risk transfer price (Ragatz, Handfield & Petersen 2002); for example, political instability in Syria may pose higher supply chain risks to an Australian bank. Banks can use risk trackers, such as Aon’s Political Risks Map (AON 2018), to assess and predict political risks to their supply chain operations.

2.7.4.5 Flexible coverage

Political risk management experts design risk transfer and mitigation programs that respond to various political effects and provide safeguards to protect business. Insurance can also be procured to mitigate against losses if uncontrollable risks effectuate (Cousins & Lawson 2007; Lawson et al 2009). A variety of resources could be coordinated to ensure that risk is eliminated in supply chain management. Various resources should be explored, such as technology, finance and information, which can assist organisations and firms in exploring their maximum potential for
combating supply chain risks (Dyer 1996). Dyer, Singh and Hesterly (2018) set out the factors thought to drive value creation and value capture over the supply chain interorganisational alliance life cycle.

2.7.4.6 Price and cost risk
All businesses are vulnerable to financial risk in the supply chain because of product price volatility. Exposure and vulnerability to risk can arise from commodity prices or indirect risks from other sources, such as transportation and higher energy costs. To minimise or eradicate price risks, firms can implement measures to manage the prices of the commodity. This will enhance cash flow, healthy commodity price competition and effective negotiating. Price management measures assist in ensuring that quoting, shipping and ordering prices are transparent (Hull 2012).

2.7.4.7 Finance handling and practices
The key purpose of finance handling procedures is to give transparent direction for collection of funds by defining the obligation and responsibilities of individuals in cash handling. Effective finance handling and practices ensure that there is a proper segregation of obligations, proper documentation and receipts, restrictive endorsement and safeguards for the handling and transportation of cash (Dyer 1996).

2.7.4.8 Finance strength of supply chain partners
Partnership in the supply chain is another potential contributing factor to product management risk. The type of partnership and individuals involved in the partnership play an essential role in determining the strength of supply chain management (Handfield & Lawson 2007; Lawson, Tyler & Cousins 2008; Liu 2013). A company can attain strength in the supply management process by choosing partners with a common interest as the company (Primo & Amundson 2002).
A financial institution can increase product variety by developing variants based on a common platform so as to establish an optimal product portfolio to increase performance (Scheuing & Johnson 1989). The company can use inventory management that involves partners for internal supply chain operations, inventory control, warehouse activities and quality assurance to manage and reduce risk (Monczka & Handfield 2010).

2.8 Conceptual model of financial supply chain risks

To assist in making sense of the large volume of supply chain risk literature (Ho et al. 2015), the literature on FSCR covered in this review was organised into the four major categories: demand risk, supply risk, product management risk and information management risk. These categories have also been used in previous major reviews of the literature on supply chain risk (Tang 2006; Ho et al. 2015).

In this review, similar classifications are used to conceptually organise what previous bibliographic analysis (Ho et al. 2015) has shown is a limited amount of literature relevant to financial institutions specifically, and less so for FSCR relevant to banking. In Ho et al. (2015), in addition to supply and demand micro-factors, they use the term infrastructure, which here is termed information technology, and manufacturing, which in a services-orientated financial institution context is labelled product management. Figure 2.2 shows the conceptual model organising the concepts and literature on FSCR and financial institutions. As shown in Section 2.6, there is limited research on FSCR in financial institutions. Further, previous research on FSCR and risks in financial institutions lacks comprehensiveness and depth (Fan & Stevenson 2018; Gelsomino et al. 2016; Ho et al. 2015). There is also a lack of research that has application utility (Kim, Mabin & Davies 2008) that can assist financial institutions in Australia to more effectively mitigate risk. Previous researchers (Fan & Stevenson 2018; Gelsomino et al. 2016; Ho...
et al. 2015) observe that while there is substantial research on various risk factors, these are often examined in isolation rather than jointly, with little indication of complex real-world applicability or generalisability.

Consequently, supply chain risk researchers have called for a more holistic examination of risk (Fan & Stevenson 2018; Ghadge et al. 2012; Gelsomino et al. 2016; Ho et al. 2015), as research on the joint impact of risks can lead to better understanding and management of risk. Ho et al. (2015) suggested that field and applied case studies are the methodologies best able to accommodate research that can make sense of real-world complexity in a way that offers practical risk mitigation models and understanding.

As illustrated in Figure 2.1, the conceptual model divides supply chain risk factors into four categories. These are summarised in Table 2.10, which lists what the literature has described as the potential risks to organisational performance arising from multiple supply chain factors. Collectively, these illustrate the multiplicity of supply chain risk factors that have implications for the examination, identification and management of risk (Harland 2019). This complexity raises the question for risk management practitioners of how to make sense of the multiplicity of supply chain risks they face and how to operate risk mitigation taking account of both intra- and interorganisational risk contributors (Lin & Zhou 2011). Other authors (Jereb, Cvahte & Rosi 2012) have attempted to take a more inclusive or integrative perspective by attempting to conceptually classify various supply chain risks, with the aim to provide applied guidance for risk management practitioners.
Adding to the complexity of the nature of supply chain risk is the potential contribution of risks from organisational and interorganisational relationships (Primo & Amundsen 2002). Cultural differences with other countries can affect the relational risks facing suppliers of their industries (Aquilon 1997; Monczka et al. 1998). Given the international aspects of Australian banking operations and partnerships, together with Australian multiculturalism, cultural differences and diversities are also potential sources of risk in the FSC of Australian organisations (Mortimer et al. 2015). In the next section, literature concerning the accommodation of FSCR complexity in the identification, examination and management of risk is discussed.
Table 2.10 Summary list of potential sources of risk discussed in earlier sections

Demand Operations Risk (Section 2.7.1)
- Shifting demand across time (Section 2.7.1.1)
- Shifting demand across markets (Section 2.7.1.2)
- Demand shift against products (Section 2.7.1.3)

Supply Operations Risk (Section 2.7.2)
- Supply network design (Section 2.7.2.1)
- Supplier relationships (Section 2.7.2.2)
- Supplier order allocation (Section 2.7.2.3)
- Supply contracts (Section 2.7.2.4)

Information Systems Risks (Section 2.7.3)
- Information accuracy and sharing (Section 2.7.3.1)
- Information system security and disruption (Section 2.7.3.2)
- Information availability and outsourcing (Section 2.7.3.3)
- Communication (Section 2.7.3.4)

Product Management Risks (Section 2.7.4)
- Product lifecycle (Section 2.7.4.1)
- Delivery time (Section 2.7.4.2)
- Political management (Section 2.7.4.3)
- Political risk tracker (Section 2.7.4.4)
- Flexible coverage (Section 2.7.4.5)
- Price and cost risk (Section 2.7.4.6)
- Finance handling and practices (Section 2.7.4.7)
- Finance strength of supply chain partners (Section 2.7.4.8)
2.9 Financial supply chain risk management and complexity accommodation

In the previous section, the complexity of supply chain risk was identified, and the call for a more holistic examination of risk was noted (Fan & Stevenson 2018; Ghadge et al. 2012; Gelsomino et al. 2016; Ho et al. 2015). Further, the need to use methods able to accommodate real-world complexity in a way that offers better understanding of risk dynamics was identified (Ho et al. 2015).

General approaches to complexity in organisational improvement such as Total Quality Management, Lean or Six Sigma (Mead 2008; Naor, Bernardes & Coman, 2013) were developed by applied practitioners and are limited in their capacity to encompass a holistic examination of risk. Rather, they have a focus on process to the exclusion of other organisational factors such as strategic functions (Doggett 2005; Kim, Marbin & Davies 2008). Alternatively, in the only study to have attempted a direct comparison of systems level problems solving methods used artificial investigator-designed tasks (Musa et al 2005) rather than real organisational settings.

In contrast, the capacity of the Theory of Constraints (TOC) (Goldratt 1988, 1990, 2010; Goldratt & Cox 1984; Goldratt & Fox 1986) and its methods has been described (see Section 2.9.1) as better able to meet both research and practitioner needs regarding the comprehensive accommodation of complexity in the examination, understanding and mitigation of supply chain risk (Kim, Mabin & Davies, 2008). Further, while comparisons in the literature are rare, Größler (2009) compared TOC to systems dynamics methods and approaches. Größler (2009) suggested that TOC methods are more suited to “real world” (pp. 217) settings and has more emphasis on organisational settings. Furthermore, it was suggested that another difference is that TOC has more emphasis on its methods being linked to problem solution formulation rather than just
complex system description. Nonetheless, Größler (2009) suggested that TOC related methods have much in common with systems thinking approaches.

2.9.1 Theory of constraints

The TOC is a management philosophy (Watson, Blackstone & Gardiner 2006; Naor, Bernardes & Coman 2013) that has an emphasis on organisational problem examination and solution generation. It is an approach that is focused on improving organisational performance and competitive advantage (de Souza & Pires 2010; Goldratt 1988). TOC has been extensively examined in the literature with over 1009 studies identified, but with limited studies in the application of TOC in the area of supply chain risk (Ikeziri et al. 2018), even fewer in the area of FSCR, and with no identified application in supply chain risk in banking institutions.

The TOC comprises a problem-solving method framework established in the well-known book The Goal (Goldratt & Cox 1984). The methods of the TOC that were developed became more inclusive and accommodating of organisational supply chain complexity than those of other theories at the time (Kim, Marbin & Davies 2008). The TOC methods started as an adapted version of the optimised production timetables (OPT), known later as optimised production technologies in manufacturing and production line contexts (Gupta 2003; Tulasi & Rao 2012). TOC was later adapted and applied to a large range of organisational supply chain performance risk issues well beyond the initial application to production lines (Naor, Bernardes & Coman, 2013; Kim et al. 2008; Ikeziri et al. 2018). According to Tulasi and Rao (2012), TOC-related methods have been applied in many functional areas of companies, ranging from production flow management, marketing, services and project management, to serving as a tool of logical reasoning.
According to the TOC, there is at least one factor that may cause problems within an organisational system (called a ‘constraint’), which may even affect the whole system of the business (Goldratt 2010). The theory considers every weak link within the business as significant and worth investigating so that issues that are subsequently found to constrain performance within the business can be overcome (Goldratt 2010). The effects of any weak point or link within the organisation were thought to radiate out to become a source of broader damage (Goldratt 2010), implying that these weak links should not be ignored, regardless of their size (Tulasi & Rao 2012). The TOC posits that all risk management should revolve around solving the identified problems and aim for maximum utility of resources (Goldratt 2010). The secret of any successful business lies in systematically and methodically identifying and assessing flaws and eradicating them (Goldratt 2010; Tulasi & Rao 2012).

Many businesses were reluctant to adopt a TOC approach within their organisations because they were apprehensive of new methods and continued with older practices (Mabin & Balderstone 2003). Moreover, it was misperceived that TOC only promoted the use of global or system-wide measures, rather than local measures (Mabin & Balderstone 2003), which was also considered an obstacle to adopting the TOC approach (Balderstone & Mabin 1998). According to Mabin and Balderstone (2003), the unorthodox practices associated with TOC and inflexible attitudes were the main obstacles to implementation. This highlights that the behaviour of people can operate as a constraint. Indeed, an inflexible attitude is perhaps the most significant attribute and constraint that should be considered in an organisation (Goldratt 1988). However, the methods were designed to change the perception and viewpoints of people managing a business, to enable them to become more open to change and to tolerate acceptance of mistakes, as well as to work on the organisation’s flaws so that any relevant issue could be addressed in the best possible manner. Balderstone and Mabin (1998, p. 206) explained:
The motivation for this is that if a system as a whole is to achieve its goal, it is best for the system’s individual parts to work as a team in ‘sync’ rather than at their own individual speeds.

The problem-solving approach that was first proposed by Goldratt and Cox (1984) and later to be described as the current reality tree method (Dettmer 1997) consisted of five main steps to identify sources of risk, and to develop and implement a remediation plan to mitigate the risk. First is the identification of the constraint or issue. This first step is to find and identify anything, including a person, an activity, a group, an action, a machine or any other relevant factor that might be causing problems and imposing constraints on the productivity of the business enterprise.

The second step in identifying a solution to a problem is exploitation of the constraint. Exploitation means that it may not always be necessary that the constraint is eliminated to achieve the maximum profit for the company. Rather, the best possible way might be to exploit the constraint in such a way that it can be utilised for the benefit of the productivity of the company by directing it in a positive manner (Gupta & Boyd 2008). However, if there is no other way, then the problem should be eliminated. In another case, the negativity of the problem can be reduced in the best possible manner available if it cannot be entirely eliminated.

The third step in problem resolution is the subordination of other activities to cover up the constraint. As discussed above, the flaws that might cause problems in the chains of connected items or effects that work for the betterment of the organisation are examined (Gupta & Boyd 2008). However, if a single element of a chain is defective, then the management team should attempt to avoid disruption of the entire chain. Therefore, activities should be coordinated and subordinated in such a way that their ongoing process is not disturbed in any way and the activities proceed in a flawless manner.
According to Gupta and Boyd (2008), the fourth problem resolution step is to elevate or invest in the constraint. This might involve the organisation investing in the constraint, such as investing in old machinery so that, even as a liability, some output can be obtained, or by increasing the number of staff members to derive maximum output if the problem is being caused by insufficient staff. The final step is to go back to the first step and repeat this process in order to tackle any other remaining major constraints contributing to problems.

For example, to achieve maximum profit in a production or manufacturing context through OPT, it is important to synchronise orders that are introduced to production that have been working with the whole system previously, known as the Capacity-Constrained Resource (CCR). With the CCR, the production rate is regarded in relation to the Drum-Buffer-Rope (DBR), where the *drum* is the way the rhythm is maintained, while the *rope* acts as the connection between the CCR and the release point of the materials to ensure that the new materials are synchronised with the prevalent production in a timely and systematic manner. Otherwise, disordered production may occur, which might lead to more losses (Rahman 1998).

The TOC proposes that there is always a constraint that might be hindering the prosperity of an organisation, and that this constraint may appear in any form or medium (Mabin & Balderstone 1999). Therefore, if one constraint is finally addressed, eliminated or invested in, the management team should not be complacent, but look for other issues that might still be present or arise and cause further issues within the organisation. Moreover, according to Mabin and Balderstone (1999), the definition of the goals of the organisation and performance measures should both be considered of potential relevance to constraint considerations.

Goldratt and Cox (1984) presented the methods or tools of the TOC, initially called OPT, in the form of a novel called *The Goal* by illustrating and explaining them under normal daily production
scenarios. Later, another business novel called *The Race* (Goldratt & Fox 1986) showed how these constraints can be more effectively overcome. A system was presented that addressed all these problems through a logic process called DBR, and over time, the applicability of the TOC-related methods was extended from the production floor to include most business types and functions, including service provision (Rahman 1998). The application of the TOC to services is discussed next.

### 2.9.2 The theory of constraints in the service sector

In contrast to the product manufacturing or production sector where the methods of TOC were first applied, the service sector produces services such as advice, expertise and specialised labour. Examples of the service sector include banking, insurance, healthcare and education. By way of contrast, the industrial or manufacturing sectors produce tangible products, such as cars, clothes or equipment. The service sector is a very important part of the world economy, constituting 67% of the worldwide GDP, and is a major source of employment (Castaño et al. 2013). This shows the importance of this sector to economic prosperity. The adaption of TOC to the service sector has been an important area of TOC application (Ikeziri et al. 2018; Kim et al. 2008). The TOC methods were initially designed for the industrial sector, but have been adapted to and implemented in the service sector (Ikeziri et al. 2018; Kim et al. 2008). The TOC approach to risk has subsequently been widely applied to a variety of service areas. Examples of the type of studies, the nature of the application and breath of national application are shown in Table 2.11.

Table 2.11 Studies of the application of the theory of constraints in various service sector types (compiled by author)
<table>
<thead>
<tr>
<th>Type</th>
<th>Country</th>
<th>Sector</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Descriptive</td>
<td>Portugal</td>
<td>Banking</td>
<td>Factors potentially involved in the decision to adopt the TOC approach by banking companies (Castaño et al. 2013; Moreira et al. 2014)</td>
</tr>
<tr>
<td>Case study</td>
<td>Turkey</td>
<td>Hospitality</td>
<td>Analyse and improve operations at a hotel using TP-TOC (Dalci &amp; Kosan 2012)</td>
</tr>
<tr>
<td>Case study</td>
<td>NZ</td>
<td>Health Services</td>
<td>Resolving resource and service issues in a large public hospital (Mabin et al. 2017)</td>
</tr>
<tr>
<td>Case study</td>
<td>Brazil</td>
<td>Higher Education</td>
<td>Integration and comparison of process engineering and the TP-TOC (Lacerda, Cassel &amp; Rodrigues 2010)</td>
</tr>
<tr>
<td>Case study</td>
<td>US</td>
<td>Construction</td>
<td>Improving performance in delivery and execution of projects (Lau &amp; Kong 2006)</td>
</tr>
<tr>
<td>Case study</td>
<td>US</td>
<td>Food</td>
<td>Product risks of different food companies and overcoming them with TOC (Kohli &amp; Gupta 2010)</td>
</tr>
<tr>
<td>Case study</td>
<td>US</td>
<td>Hospitality</td>
<td>Café operations improvement in a café (Reid &amp; Cormier 2003)</td>
</tr>
</tbody>
</table>
2.9.3 Tools for identifying risk mitigation targets

The TP methods employed in the TOC are intended to enable the user to map, identify, analyse and implement solutions for organisational problems, including supply chain risks (Goldratt 1990; Mabin & Balderstone 2003). TP methods have as their basis a process for developing cause–effect–cause diagrams, which aim to elicit feasible explanations on why things happen, instead of how they happen.

The TP provides for the establishment of a method to identify and remove observed UDEs arising from the constraints that together negatively affect organisational performance (Cox et al. 2012). Kim, Mabin and Davies (2008) reviewed studies on the organisational application of TP, but application to the banking sector is limited. For example, Moreira et al. (2014) discussed banking in Portugal in a review of TOC application to services, but did not apply TOC-related methods to specific bank cases. Instead, Castaño et al. (2013) and Moreira et al. (2014) provided commentary on how TOC might be of potential benefit if applied to banking organisations, based on findings from other service industry applications.

2.9.4 The contribution potential of the TOC in the banking sector

In the banking sector, the foremost constraint proposed is the dissatisfaction level of customers (Castaño et al. 2013), the group that mainly drives the banking sector towards prosperity. If people are not content with the services of the bank, losses may result (Chigamba 2011). This occurs mainly because customers choose alternatives for the provision of financial services. With globalisation, there has been an increase in the profitability of the banking sector. Chigamba (2011) noted that banks are constrained by competitive pressures and a rapidly changing environment and need to attract and retain customers if they want to survive and prosper. The
literature indicates that the TOC approach and TP methods show promise for application to banking service provision in Australia.

Many constraints are caused by customer dissatisfaction and linked to risk in banking service provision (Castaño et al. 2013; Moreira et al. 2014). Moreover, bank lending is often constrained by the availability of insured deposits (Jayaratne & Morgan 1997), which can lead to reduced ability to meet customer demand for finance. Such customer dissatisfaction problems have been analysed within non-financial sectors, but still require investigation in the case of banks.

Negative publicity about banks (e.g., Commonwealth of Australia 2018; Withers 2018) may influence customer dissatisfaction, which in turn, may contribute to losses for the sector if people begin to look for alternative financial services that they consider more trustworthy and efficient (Mateso 2014). Further, it has been shown (Valverde, Fernández & Udell 2008) that banking constraints are increased if transactions are carried out by firms that are unconstrained and that have not been fully checked by the banking sector or verified as appropriate before they are accepted by the bank as clients. Moreover, research has shown that investment is sensitive to bank loans for unconstrained firms but not for constrained firms, while trade credit predicts investment, but only for constrained firms (Valverde, Fernández & Udell 2008). According to Valverde, Fernández and Udell (2008), monetary shocks, such as the 2007 global financial crisis, show that there is a need for the banking sector to manage the problems that might be contributing to negative influences and losses.

Banking efficiency is significant not only in the banking sector, but also for the development of the country, as the economic conditions of any nation depend largely on how appropriately banks are functioning (Matthews 2010). In that sense, risk reduction in the banking sector is important
to the extent that it can help prevent the occurrence of economic risks for the bank (Matthews 2010, p. 2):

The efficiency of banks, relates to the efficiency of the banking market, which in turn relates to the efficiency of the intermediation process and the efficiency by which monetary policy passes through to bank lending.

However, despite the importance of knowledge of risk and risk reduction in the banking sector, there is limited application of TOC-guided risk reduction research and the application of TP methods in the banking sector. Despite searching for studies that might demonstrate application of TOC or TP methods in the banking sector, only a limited number of studies (Bramorski, Madan & Motwani 1997; Castaño et al. 2013; Moreira et al. 2014) were found, and these did not apply methods, but rather conceptually examined the hypothetical application potential of TOC to banking.

Castaño et al. (2013) and Moreira et al. (2014) analysed which elements of the TOC to best apply to the banking sector. The preliminary research revealed that there were four elements that could be used within the banking sector: throughput, inventory, operating expenses and constraints. These elements strongly correspond to the capital gained from services provided to consumers, the capital needed to create profit and the money used to fund investment, as well as the constraints that occur within all activities of the banking sector (Castaño et al. 2013; Moreira et al. 2014). Moreover, Castaño et al. (2013) and Moreira et al. (2014) considered the following factors in the banking sector:

- Tools or software that can enhance development;
• Attributes of the banking sector that differ from those of other business systems, such as the changing attitudes and choices for consumers;

• The rapid changes in the banking industry;

• The leadership required for the various changes; and,

• The commitment of those who work within the entire organisation.

Modern technologies, including smart phones, tablets and computers, have radically changed the management systems in various fields worldwide; while they bring benefits, they also bring risks to banking (Jalil, Talukder & Rahman 2014; Talukdar, Quazi & Sathye 2014). The banking system now employs these once-emerging technologies extensively, and most portable devices have banking-related ‘apps’ (software applications) available for consumer use.

As shown in the literature (e.g., Ikeziri et al. 2018), manufacturing companies have successfully made use of TOC-related methods to assist in risk reduction and performance improvement, but the banking services system still needs to interpret and adapt this research for application to practice for it to benefit. According to Bramorski, Madan and Motwani (1997), customers who provide the bank with deposits that contribute to inputs often use the same bank to meet their needs for loans, which directly contributes to the bank’s output. Customers of a bank tend to use that bank for multiple financial services. For example, Bramorski, Madan and Motwani (1997) described a bank in the midwestern region of the US which realised that the mortgage system often took a long time. Hence, the bank decided to implement the TOC to identify and resolve the problem. It was discovered that there were two kinds of customers: one that paid 20% or more for their home mortgage insurance and another that paid less than 20%. Analysis of the latter group revealed that the bank took too long to carry out the whole process of employment, research and feedback survey (Bramorski, Madan & Motwani 1997). The bank then decided to follow the other
steps of the TOC. New techniques were developed for obtaining and verifying information, and applicants were asked to bring alternative documents for the validation process. This development was very important for the bank because it began to apply this framework to other issues as well. This case illustrates the potential for the application of TOC-related methods in banking to improve performance and reduce risks in the supply chain (Bramorski, Madan & Motwani 1997).

While many authors have investigated the application of TOC-related methods in various service sectors (e.g., consultancy, education and health) (Ikeziri et al. 2018), only three investigations were found that considered TOC in relation to banking services. Mabin, Forgeson and Green (2001) illustrated the use of TOC methods in a single NZ banking case study but the focus of the examination was on change management rather than risk management or the supply chain. Castaño et al. (2013) and Moreira et al. (2014) conceptually examined factors explaining why banks might adopt the TOC framework in the Portuguese banking sector, and Bramorski, Madan and Motwani (1997) described the use of the TOC to identify a banking organisation’s goal and detect the constraints to achieving enhanced performance. The constraints in these banks examined only selected attributes such as policies and procedures, which might typically be found in a TOC approach to an organisation’s operation as a whole. In both instances, only selected attributes were examined and neither undertook a comprehensive or systems view of banking operations where TP methods were applied. Reid (2007) provided a fictitious conceptual example of a bank to illustrate the potential application of the TOC to the banking service sector. With only preliminary conceptual approaches tested, none of previous publications on banking used the TP methods to assess, analyse and create solutions in case-based applied research.

In summary, despite widespread research in a variety of industries, research on the application of TOC has been comparatively limited in the financial services sector, and is non-existent in
Australian financial institutions. The application of TOC is demonstrated by the literature (Ikezeri et al. 2018) to have the potential for risk identification and reduction and to have application potential to identify, analyse and reduce risk in Australian financial institutions.

2.10 Conclusion

This chapter reviewed the literature on financial risk from a supply chain perspective with an emphasis on financial institutions. The literature review found three main themes. First, a very large range and diversity of supply chain risks have been identified and described in the literature. Second, the literature showed sources of risk are complex and multifaceted and include organisational relationships with suppliers and customers, technology risks and product management risks. This literature provided the foundation for a conceptual model to organise risk in a financial institution context. Third, supply chain risk management and research showed that methods related to the TOC are useful because they can accommodate risk complexity, where multiple factors can be examined jointly through a holistic organisational perspective. The literature indicates that the application of TP methods to banking FSCR has potential to assist in risk identification, risk analysis and solution options.

While the TOC has been extensively applied in a number of industries, there has been a limited conceptual examination of the benefits of the application of TOC or related methods in banking, and none in Australian financial institutions. The literature illustrated the factors that form the basis for a conceptual model to make sense of supply chain risk in Australian financial institutions. The model includes four main types of risk: demand management, supply management, product management and information management. The next chapter describes how the research questions will be addressed. The questions are what FSCR are identified as currently present in Australian financial institutions? (RQ1); what is the nature of the causal relationships among the FSCR that
adversely affect financial institution business functions? (RQ2); and what future risk control practices could mitigate FSCR in Australian financial institutions (RQ3)?
CHAPTER 3

METHODOLOGY

3.1 Introduction

The purpose of this chapter is to describe the research methodology adopted in this research. It explains the research strategy used and the steps followed to meet the research aims, through the application of the research strategy. Section 3.2 describes the paradigm that forms the basis of the methodological framework and that is utilised to address the objectives of this study. The methodology employed is then described in Section 3.3, including how the research questions are to be answered. Section 3.4 gives an explanation of how the cases were sampled and the selection of participants. Section 3.5 describes the structure and design of participant interviews and the interviewing process. Finally, Section 3.6 describes reliability and validity considerations, and ethical considerations.

3.2 Research paradigm

This section describes the underlying assumptions of the research paradigm adopted for the present study. This makes explicit the principles of inquiry that shape the nature and approach in the selection of an appropriate methodology to address the research questions and the nature of the phenomenon under investigation.

A research methodology is a systematic approach of inquiry to be followed in solving a specific research problem (Kothari & Grag 2014). It describes the series of phases through which the research progresses to meet its objective, such as data collection, data analysis and data interpretation (Creswell & Plano Clark 2011; Hall & Howard 2008). In addition, the research
methodology explains various methods and techniques that could be used in each phase of the research and which methods are most suitable for the relevant research (Kumar 2005).

The selection of a suitable research methodology depends on the nature of the research (Srivastava & Thomson 2009). There are two main types of research: exploratory research and confirmatory research (Boudreau, Gefen, & Straub 2001). A research project of an exploratory nature generates insights by analysing and developing understanding about the responses to a phenomenon of interest (Jaeger & Halliday 1998). Such research requires data to be collected and analysed, with insights gained by interpreting the data.

According to Guba and Lincoln (1994), various interpretations, by both the researcher and participants, are involved in a study, and differences in interpretation are further reflected through the viewpoint of the reader, as well as other contextual influences. The paradigm underlying the researcher’s choice of methodology is influenced by a range of philosophical perspectives. A paradigm comprises a set of assumptions regarding ontology, epistemology and methodology (Guba & Lincoln 1994). The paradigmatic assumptions guide the selection of the methodological approach that is best matched to the characteristics of the research questions and the nature of the phenomenon under investigation. An adopted research paradigm is ‘a set of fundamental assumptions and beliefs as to how the world is perceived which then serves as a thinking framework that guides the behaviour of the investigator’ (Wahyuni 2012, p. 69). In addition, Guba and Lincoln’s (1994, p. 107) description of a paradigm asserts that it is shaped by the beliefs about an experiential schema that the investigator brings to how the research inquiry is constructed:

A set of basic beliefs that deals with ultimate or first principle which represents a world view that defines, for its holders, the nature of the ‘world’, the individual’s place in it, and the range of possible relationships to that world and its parts.
In describing the rationale for the selection of the methods, the relationship between the paradigmatic assumptions and the adopted methodological design are best made explicit so that these can be assessed for evaluating the appropriateness of the methods chosen and so that the limitations of the findings of the investigation can be better understood.

Confirmatory research (Boudreau, Gefen & Straub 2001) is typically conducted in accordance with a positivist tradition (Popper 1959); an inferential approach is taken to test hypotheses about potential causal relationships between a chosen set of variables (Milam 1991). In contrast, this study utilises an interpretive exploratory approach, which is deemed the most appropriate considering the objectives of the study outlined in Chapter 1. Interpretivism suits the nature of the research questions posed in this study, which aim to explore how complex organisational supply chain risk characteristics and determinants operate in financial institutional contexts. An interpretive view is necessary because a detailed investigation into complex real-life social phenomena involves the interpretation of subtleties and ambiguities attached to the ideologies underpinning such practices (Graham 2010). Further, rather than decontextualising an arbitrarily selected subset of variables for investigation, an interpretive study may seek to make sense of real-life settings of phenomena, where much of the potential influences are jointly taken into account. A qualitative approach is considered essential in a financial institutional case study, as in this context actions and behaviours of different key institutional actors shape and are shaped by multiple factors, and these are difficult or unfeasible to quantify and measure with the precision of positivist-based methods (Nilphan 2005).

Wahyuni (2012) commented that the interpretivist paradigm is based on an ontology where the nature of reality is assumed to be both socially constructed and subjective. Interpretivism as an epistemology implies the need for interaction and dialogue between the investigator and study
participants (Wahyuni 2012). Epistemological interpretivism requires an interpretivist investigator to ‘focus upon the details of the situation, the reality behind these details, subjective meanings and motivating actions’ (Wahyuni 2012, p. 70). Interpretivism as an epistemology assists the researcher in interacting with study participants in a complex social science phenomenon (social inclusion practices), and focuses on how social interpretations and interactions can be influenced by their frames of reference (Denzin & Lincoln 2000).

An interpretive paradigm assumes that participants’ construction of organisational social realities and how they make sense of meaning is an important task of inquiry. Therefore, an objective discovery of the world and how it is observably linked to underpinning theoretical causes is unnecessary. As a result, researchers within the interpretivist paradigm acknowledge that a total understanding of any particular social reality is not achievable. This is particularly so when the purpose is to try to make sense of a highly complex organisation and interorganisational system of multiple components and processes, which may, in turn, vary from applied setting to setting, and from time to time.

3.3 Methodology

Based on the paradigmatic assumptions underpinning this study described in Section 3.2, an inductive approach has been utilised in the study process, where participant interview data are iteratively shaped to make sense and derive a more developed understanding of the complex phenomena under investigation. Therefore, this study adopts a qualitative inquiry based on an interpretivist assumption with an aim to uncover contextual knowledge about the perceived influences on financial institution risk related phenomenon. In the case of organisational supply chain risks described in Chapter 2, the phenomena under investigation are complex and interacting, and are located in organisations with similarly complex characteristics. This requires
a methodology that can examine multiple supply chain risk determinants jointly, and which can accommodate causal complexity.

The next section provides a description of the methodology and its design. It provides further justification for the selection of a qualitative study as the methodology to address the study questions. This is followed by an explanation of the appropriateness of selection of case studies as the study design (Scotland 2012).

### 3.3.1 Qualitative multi-case studies

To enable an understanding of risk-related phenomena in financial institutions, a qualitative case study methodology was chosen for this study because of the match between the exploratory nature of the inquiry posed by the research questions and the nature of the answers that a qualitative method seeks to discover.

Real-world risk-related phenomena, as they occur in complex organisations, can be understood, explored, described and interpreted by applying a qualitative case study method because this enables a holistic understanding and explanation (Al-Busaidi 2008) where multiple variables are considered jointly rather than in isolation. In addition, a qualitative case study permits an in-depth investigation into how people interpret and make a case of specific circumstances, and this assists the investigator in probing the underlying complexity, which cannot be as well accomplished with quantitative methods of inquiry (Matveev 2002). Therefore, a qualitative case study inquiry employs tools and strategies (such as interviews and observations) to enable making sense of the inherent complexity of supply chains related to service-orientated financial institutions. These tools and strategies are deemed relevant where the study questions are exploratory in nature, such as those accessed by how and why questions (Yin 2017).
Yin (2014, p. 13) argued that the use of case study inquiry ‘copes with the technically distinctive situation where there will be many more variables of interest than data points, and as one result relies on multiple sources of evidence, with data needing to converge in a triangulating fashion, and as another result benefit from the prior development of theoretical positions to guide data collection and analysis’. The advantage of adopting a case study approach is that there is no specific data collection or analysis method; rather, a variety of methods can be used in conjunction to provide triangulation and rigour (Patton 1999; Yin 2014). This makes the case study approach a comprehensive research strategy (Yin 2017).

Although there are many advantages associated with the adoption of case studies as a research method, there are also many criticisms. Case studies typically make use of only a few examples to represent a wider range of examples being investigated, and the credibility of these generalisations is often criticised (Yin 2014, 2017). Further arguments suggest that case studies should not be limited to just one case, but instead generalised to similar cases because there are similar influences operating on the same case types, as even though each case may be a separate entity, it may share common contexts (Yin 2014, 2017). For example, different banks and risk management practitioners have certain contexts in common, such as shared business types, strategic objectives and regulatory contexts, as well operating from a shared risk management knowledge base.

Eisenhardt (1989) defined the case study approach as a study strategy that seeks to develop an understanding of the complex dynamics present in real-life settings. The application of a case study design is suited when employing questions such as ‘how?’ and ‘why?’. The case study design is suited to this type of understanding and, accordingly, is also suitable when an in-depth
and comprehensive investigation is required to comprehend a complex issue (Yin 2014). Section 3.3.3 describes the nature of the how and why questions used in the current study.

A multiple case study approach is used in this research, because it is useful to explore multiple cases in natural settings for the purpose of obtaining in-depth knowledge, where what is found may be applied collectively. A multiple case study design allows for validation of understanding, on the assumption that the different cases selected exhibit differences in resolution (Yin 2014, 2017). A case, in the context of a method of inquiry, can be defined as ‘a phenomenon of some sort occurring in a bounded context’ (Punch 1998, p. 119). Further, the trade-off in case study methodologies between depth and generalisability is mitigated to some extent where multiple cases are used rather than a single case.

Case studies can be grouped into three main categories: the intrinsic case study, the instrumental case study and the collective case study (Stake 1995). An intrinsic case study aims to enhance an investigator’s understanding of a specific case undertaken or when ‘we have an intrinsic interest in the case’ (Stake 1995, p. 3). The instrumental case study, conversely, aims to enhance a researcher’s understanding of a particular issue by using a specific case as a medium. Stake (1995, p. 3) claims that an instrumental case study as a method of inquiry is necessary when there is ‘a need for general understanding, and [we] feel that we may get insight into the question by studying a particular case’. Last, a collective case study is an extension of the instrumental case study, where the main objective is to include multiple cases for better insight into a certain phenomenon or population (Punch 1998). Therefore, a collective case study implies ‘important coordination between the individual studies’ (Stake 1995, p. 3). This allows for the development of a common understanding applicable or generalisable to each of the participating cases. While Stake’s (1995) may not be mutually exclusive, this research best fits the collective case study category as it
involves studying multiple cases simultaneously in an attempt to generate a consensus appreciation of the risk-related issues under investigation.

A multi-case study approach is also justified on the basis of its aim of exploring the strategic approach of financial institutions to enable potential adaption arising from the common understanding so developed, to further understand what changes are required to transition from the current state to a more desired future state. The strategy that guides this adaptive change is similarly developed from the multi-cases to develop a shared understanding through iterative cross-case validation. Further, in the banking sector, a case study approach is considered beneficial because it allows the investigator to examine both the micro and macro issues affecting the decision-making aspects of the key policy participants of the respective institutions (Ruddy 2008). Leisyte (2007) claimed that the case study method is best used when aiming to include consideration of contextual conditions that might be highly pertinent to the phenomenon of study.

According to De Vaus (2008, p. 252), a comparative cross-national study design, structured on a multi-case basis, utilises a ‘cultural and interpretive model in that it is taken for granted that any behaviour, attitude, indicator or effect can only be understood within its historical, cultural and social context’. This implies that a specific understanding of organisational practices can be appreciated in accordance with a specific set of historical, cultural and social contexts. Further, it was argued that a study of an organisation should be comparative as a result of factors, such as institutional dynamics, that shape the nature of industry sectors across different regions and countries under investigation (March & Olsen 1998; Ruddy 2008; Välimaa 2008).

Bryman (2004) presented a comparative inquiry that employed multiple methods of probing conflicting cases. In a collective, multi-case study design, a comparative inquiry enables a more diverse and richer understanding of a social phenomenon when it is conducted with two or more
conflicting cases (Bryman 2004; Pauwels & Matthyssens 2004). A comparative inquiry has been undertaken in a previous study focusing on the policy issue of equity and widening participation practices of selected public higher-education institutions (Graham 2010). In the context of this study, policy frameworks are thought to be able to shape the social inclusion practices of the selected group of financial institutions in Australia.

3.3.2 Analysis method: thinking process of the theory of constraints

The procedural and analytic approach usually adopted for the analysis of case study interview data is often some variant on thematic content analysis (Braun & Clarke 2006; King, Horrocks & Brooks 2018; Vaismoradi et al. 2016). The methods of thematic content analysis usually comprise the interview process and transcription, interview content coding, content categorisation and thematic analysis, all of which are largely atheoretical. Theory or a researcher’s conceptual frame of reference may influence the specific interview question content formulation, the type of interview data coding adopted, and the selection of theme content construction and interpretation (Braun & Clarke 2006; King, Horrocks & Brooks 2018). Instead of thematic content analysis as it is usually applied (King, Horrocks & Brooks 2018; Vaismoradi et al. 2016), this research elicited and analysed participant interview data using TOC methods such as the TP (Goldratt 1988, 1990, 2010; Goldratt & Cox 1984; Goldratt & Fox 1986). This differs from a thematic content analysis in a number of ways. First, it was developed specifically in the context of organisational problem solving where the aim is not simply to identify, describe and interpret themes, but to identify underlying causes of organisational problems and develop solutions (Mabin & Balderstone 2003; Rahman 1998). Second, it adopts a method of participant inquiry characterised by a more interrogative or investigative dialogue rather than passive recording and coding of participant responses to questions methods (Goldratt 1990; Kim, Mabin & Davies 2008; Mabin &
Balderstone 2003). Third, how interview data is formulated to construct the examination of problems and solutions is largely theoretically pre-defined rather varying on a study-by-study basis (Naor, Bernardes & Coman 2013). As described in Section 2.9, Goldratt (1999) developed the TP specifically as an organisational problem diagnosis, management and mitigation approach. Fourth, commentators (Mabin & Balderstone 2003; Ikezeri et al. 2018; Rahman 1998) have argued that the TP of the TOC is a promising approach that can ultimately lead to more effective, successful and long-lasting organisational objective attainment. This section describes the approach, its suitability and proposed application to the case studies under investigation.

The use of TP in this research offers more than issue or theme identification or risk assessment; it offers a way to develop a remediation and solution implementation approach that provides a basis to formulate remedial financial institution risk reduction strategy to change outcomes. This approach was novel in it application to financial institutions in that it uses complex process mapping rather than simple theme description typical of case study approaches more generally. Furthermore, the process mapping was illustrated though whole organisation visualisations.

The TOC posits (Goldratt 1988, 1990, 2010; Goldratt & Cox 1984; Goldratt & Fox 1986) that organisations can be assessed and controlled by variations on three measures: throughput, operational expense and inventory, where the latter refers to all the money that the system has invested in purchasing items that it intends to sell (anything from equipment to people and policies). As described in Section 2.9, reviews of TP aspects of the TOC have described its history and development and the major components of the TP (e.g., Mabin & Balderstone 1999; Ikeziri et al. 2018).

The financial industry is typically involved in scenarios where systemic or external risks affect the whole sector, such as the global financial crisis or other economic shocks. Although the effect
of systemic risks cannot be ignored, this research study examines the effectiveness of the TP in solving the controllable internal risks that affect operations internally and the interfaces with its customers and suppliers in the financial supply chain. As described in Chapters 1 and 2, most supply chain risks in financial institutions lend themselves to being defined as FSCR, as all supply chain risks in these types of financial service organisations either directly or indirectly have financial-related characteristics.

3.3.3 Description of the application of TP methods to the case studies

The TP (Goldratt 1988, 1990, 2010; Goldratt & Cox 1984; Goldratt & Fox 1986) typically focuses on solving the current problems facing companies in the financial sector. The senior risk manager participants in the case study interviews considered the questions posed by the investigator, which were based on the TP methods, to describe the nature of the current situation.

The first TP (Goldratt 1990; Kim, Mabin & Davies 2008; Mabin & Balderstone 2003) technique question used in the application of the methodology is ‘What to change?’ This question prompts the participants to rethink and dissect the operations to identify the problem at hand. For instance, the participant is asked to determine the weaknesses that may lead to decreased customer satisfaction by asking themselves what has to change. The second question is ‘What to change to?’ This question helps to define the desired situation. Most banking companies have an objective of reaching as many customers as possible. The final question is ‘What causes the change?’ This means that the company has to determine the specific measures needed to achieve the desired effects. The TOC thus encourages a perceived cause-and-effect analysis of the situation, from the current state to a desired future state.
In summary, the TP is a method that seeks to answer three main questions relating to the overall purposes, which is to identify, examine and remove ‘constraints’ (Goldratt 1990) that inhibit the attainment of organisational objectives. These core questions, their purpose and the matching TP tools designed to answer them are shown in Table 3.1. Next, further detail of the TP methods are described.

<table>
<thead>
<tr>
<th>Question</th>
<th>Purpose</th>
<th>Tool</th>
</tr>
</thead>
<tbody>
<tr>
<td>What to change?</td>
<td>Identify core issues</td>
<td>Current reality tree</td>
</tr>
<tr>
<td>What to change to?</td>
<td>Develop practical recommendations</td>
<td>Evaporative cloud</td>
</tr>
<tr>
<td>How to cause the change?</td>
<td>Implement solutions</td>
<td>Future reality tree</td>
</tr>
</tbody>
</table>

3.3.3.1 The thinking process as an analytic tool

The TP is a method where the objective in application to cases is to solve organisational problems. The TP is used to examine the situation and develop a map for the process needed to achieve the objectives of problem remediation (Kohli & Gupta 2010). The aim is to solve unstructured or ill-defined problems and to identify cause-and-effect relationships that may generate constraints (Mabin & Davies 2010).

Through application of the TP method, the participants, in collaboration with the investigator, validate successive iterations of inquiry and develop an aggregated participant consensus view about how organisational strategic objectives are pursued and better achieved. The TP is applied to develop a view about the determinants of the problem and the possible solutions. The problem resolution alternatives are listed and the resources to achieve the objectives are itemised. Through the TP methods, the participants select the best alternative. The most common TP method used to
identify the alternatives is a cost–benefit inquiry. The final step is the application of the
determined alternative, followed by examination of the processes of risk monitoring and control.

3.3.3.2 Identification of the undesirable effects

UDEs refer to those issues in an organisation that lead to loss or failure within the business. This
TP terminology points towards the effects that are undesirable in an organisational system, a
process or its stakeholders and clients (Hohmann 2015). UDEs are thought to limit the
performance of an organisation and often reduce the prosperity of a company to a marked extent.
According to the TP, UDEs include issues that are obvious to people and therefore easily
identifiable as detrimental. What is noteworthy about this notion is the fact that the effects are
easily seen by everyone; however, the root cause of these effects may not be obvious to
management. Therefore, while UDEs are often clearly visible, the underlying or root causes may
not be visible. The TP methods are designed to reveal these root causes and to identify which are
most important or have the most causal influence on the problem. If the underlying or root causes
or issues or constraints can be eliminated, the UDEs should be resolved. Therefore, it is important
to first identify the UDEs. If all the issues that influence the chain of smooth effects resulting in
success are identified, their influence can be controlled to a greater extent (Taylor & Ortega 2003).
Figure 3.1 illustrates how UDEs are mapped in the methodology to create a diagram that depicts
a model of risk causality called a CRT.

This diagrammatic representation of causal pathways forms the basis of CRT and was devised in
the TP as a tool to assist to visualise and solve problems in organisations. For instance,
institutional managers who face a competitive disadvantage in the market may employ the CRT
to dissect the present limiting conditions as stipulated by the TP, followed by examination of
possible solutions, such as advertising their products more aggressively.
Figure 3.1 Illustration of the identification and perceived causes of undesirable effects and identifying the ‘what to change’ part of the TP method.

Legend:

**UDE** Undesired Effect

**Core Problem** Underlying core problem that causes the undesired effects that arise from it.
Notes: Starting with the UDEs and available knowledge, the TP enables an analysis where case study participants through integratory dialogue pinpoint the core problem. The green circles signify combined effects of more than one influence.

3.3.3.3 Current reality tree construction process method

The CRT is a TP diagnostic method that identifies factors in the current state of business functions thought to contribute to the problems of concern (Goldratt 1990). The application of this method reveals the current situation of the organisational system; it was defined as the logical structure planned to depict that state of reality as it currently exists in a given system (Goldratt 1990). The CRT shows perceived causes and effects, given a specific set of circumstances. It is constructed by the participants top-down, from observed UDEs (see Section 3.3.3.2) to postulate likely causes of those effects (hence the term effect-cause-effect). Figure 3.2 shows an example of a CRT showing the UDEs collectively caused by a core problem. TP assumes that there are interdependencies between the UDEs, and that there must be a common cause or core problem underlying all of these (Ikezeri et al. 2018).

The process of preparing a CRT uses the logic of cause-and-effect relationships through the application of the TP. Goldratt (1994) explained the following six steps in the formation of a CRT:

**First.** The management team determines the extent to which the problem affects the company operations and identifies all the participants who will be involved in finding a solution to the problem. The company might be experiencing a low customer base that affects the company’s profitability. Management lists all the affected parties, such as the marketing department, the human resource department and the top management, who might be using obsolete strategies.

**Second.** Identify and listing all the relevant UDEs. An ideal list consists of no more than 5–10 undesirable effects—more than that implies too much detail at this early stage. The
greater the number of UDEs listed, the more the problem needs to be simplified. Complex problems are relatively hard to solve; management must simplify the problem to solve it without ignoring any details. For example, a banking service provider with a low customer base will list all UDEs, which might include the following: low profitability of the banking business, unsatisfied customers after being served and low numbers of loyal customers.

**Third.** Mapping all the UDEs in a diagram showing the cause-and-effect relationships between the entities. A low customer base is known to cause low profitability but is caused by other factors such as low customer satisfaction or a highly competitive market. The company analyses each and every UDE listed to link it with a possible cause-and-effect relationship to ensure that the complexity of the problem is simplified.

**Fourth.** Review and revision of the mapped UDEs to ensure that there is clarity and completeness in the cause-and-effect relationships. The diagram has to be clear and complete to ensure that every aspect is included. The clearer the CRT, the simpler it is, facilitating determination of a solution (Mateso 2014).

**Fifth.** Determination of the cause of the UDEs and what is affected by the UDEs. In the case of a low customer base, the management determines what UDEs the low customer base causes and what might have caused this.

**Sixth.** Identification of the core causes. Management analyses all the UDEs and determines the root cause of these effects. The company will be able to solve the problems by eliminating the core causes. For instance, management might reveal that a low customer base is caused by poor customer service provided by the human resource department and that all the other UDEs arise from that particular root cause. Management will therefore take the necessary steps to improve the services provided to customers, thereby resolving all the UDEs.
Application of the CRT facilitates recognition of cause-and-effect relationships in the current structure of a business to solve the problems at hand (Goldratt 1994). According to Dettmer (1997), and illustrated by the arrow connectivity in Figure 3.2, the CRT also provides for the visualisation of the effects of potential feedback loops—the loops can open up more possibilities for the location of remedial action within the functional map provided by the CRT. Using a human resource example, the proposition of improving the human resource department may affect various departments, with both desirable and undesirable effects, including feedback loops. The use of the CRT tool enables formulation of alternatives and correcting methods when such incidences are identified and enable a complex systems-orientated view (Dettmer 1997).

3.3.3.4 Future reality tree construction process method

The TP FRT technique is intended to assist in overcoming the challenges facing participants regarding how to identify barriers that prevent addressing the cause of a problem. The FRT method seeks to create awareness of solutions to a problem by utilising the logic previously developed in the CRT. The FRT is similar to the CRT, but the hypothetical solutions or actions with potential to transform an undesired effect into a desired effect are identified and placed within the tree diagram to illustrate possible future solutions for the issue and to describe a desired future state (Balderstone 1999 Dettmer 1997; Hohmann 2015; Kim, Mabin & Davies 2008). It helps in solving the ‘What if?’ questions that arise when a new operation with a remedial purpose is introduced into a system. For instance, if excessive operational costs are identified by the TP CRT, management may take various steps to reduce costs, which will affect the current reality structure and also have future effects.
The FRT identifies possible steps to eliminate the effects caused by the introduction of new processes in the future (Hohmann 2015). The cause of the new challenge is an effect of the new process introduced in the company structure. In short, the FRT proposes a process for management to consider how to deal with future problems that may arise as a result of new processes introduced into the organisational system.
3.3.3.5 Steps in preparing the future reality tree

The FRT is constructed from the CRT (Balderstone 1999; Dettmer 1997; Hohmann 2015; Kim, Mabin & Davies 2008). The CRT helps in identifying the root cause of the problem from the UDEs. The CRT example used above identified poor service provision by the human resource department as the root cause of the low customer base. Construction of the FRT begins at this stage. The FRT portrays the use of ‘injections’—items or actions that are new or done differently to neutralise the effects of the UDEs and convert them into desirable effects (Balderstone 1999; Dettmer 1997; Hohmann 2015; Kim, Mabin & Davies 2008). The UDEs are exchanged with desirable effects (DEs) through the application of injections.

Figure 3.3 shows how injection solutions are used in FRTs to change the UDEs to DEs. The scenario of the poor service provided by a human resource department can be changed through a variety of solutions (e.g., good remuneration, job training and good supervision) to high-quality service provision. The first step is to identify a list of possible solutions or injections. The second step is solving the problems by finding the best possible solutions to the core problem (Balderstone 1999) and testing solution options to determine the best potential solution effectiveness (Dettmer 1997).

The third step involves a combination of injections and providing the solution for the problems and mapping them into a single diagram (Balderstone 1999; Dettmer 1997; Hohmann 2015; Kim, Mabin & Davies 2008). Figure 3.4 is an illustration of a FRT that shows the future state that the company desires to achieve. For example, the FRT shows the possible ways in which the company can deal with the problem of low customer satisfaction and the desired future state of a highly competent human resource department. The injections that transform UDEs (shown in a CRT) to
DEs (shown in a FRT) are conditions or processes that do not yet exist, but are intended to be implemented in the future to achieve the desired future state.

Figure 3.3 Use of an injection or solution in future reality trees to convert causes of undesirable effects into desirable effects

Goldratt’s (Dettmer 1997) categories of legitimate reservation provide guidelines for communicating reservations about the validity of the elements and connections within the trees (Balderstone 1999; Dettmer 1997). The FRT serves the following purposes (Dettmer 1997):

1. Enables effectiveness testing of new ideas before committing resources to implementation;
2. Determines whether proposed system changes will produce the desired effects without creating negative side effects; reveals through negative branches whether (and where) proposed changes will create new or collateral problems as they solve old problems, and what additional actions are necessary to prevent any such negative side effects from occurring;
4. Provides a means of making beneficial effects self-sustaining through deliberate incorporation of positive reinforcing loops;
5. Provides a means of assessing the impacts of localised decisions on the entire system;
6. Provides an effective tool for persuading decision-makers to support a desired course of action; and,

7. Serves as an initial planning tool.

Figure 3.5 shows a summary of the research analysis process involving three phases of the TOC TP methods. First, a CRT is constructed showing the current undesirable outcome arising from the UDEs. Second, from the CRT data, and devising and testing injection solutions with the participants, a FRT is constructed where the proposed injections convert UDEs into DEs. The undesired outcomes shown in Figure 3.5 represent the cumulative effect of multiple UDE’s have on posing risk or attenuating the achievement of organisational corporate objectives or the capability to attain the mission of the organisation. An intermediate objection may relate to the objective of an organisational division or sub-business of the broader business. Desired outcomes represent the cumulative effect of injections applied to created multiple DE’s that improve the achievement of organisational objectives and the attainment of the organisational mission. Both of these effects on organisational outcomes relate to an entire perspective of the organisation. Last, to illustrate how the finding might be translated into risk management practice, plans for how the injection might be implemented in practice are discussed.

In summary, the process of inquiry with the participants uses TOC TP methodologies to construct current reality trees that represent a consensus view informed by the characteristics of the case study financial institutions, and representative of banking institutions more generally. These then form the basis for future reality tree construction and the generation of solutions to risk and the formulation of risk mitigation approaches suited to Australian financial institutions.
Figure 3.4 Illustration of the future reality tree (FRT) showing locations of injections (solutions) to create desirable effects (DEs).
Figure 3.5 The research analysis process summarised as first CRT construction, followed by FRT construction and the use of the FRT and injections in risk management plan implementation.
3.4 Data collection procedures

The procedures are informed by the literature regarding TP methods, the FSCR conceptual model and participant data respectively. As discussed in Section 3.3.1, having corroborating sources of data is pertinent to obtain a robust understanding of the risk phenomenon investigated. As described in Section 3.2, the data collection methods used to frame the focus of the study are in accordance with the selected paradigm, the objective and the research questions.

3.4.1 Data collection sample

According to the register of the Australian Prudential Regulation Authority (APRA) (2018), there are currently 147 authorised deposit-taking institutions in Australia. These institutions are categorised by market capitalisation into three tiers: Tier 1, 2 and 3 (Gorajek & Turner 2010). Tier 1 represents financial institutions with the largest capitalisation, Tier 2 represents medium-sized institutions, and Tier 3 represents small institutions.

It was decided to stratify the sample through a selection of different-sized financial institutions, one from each of the three tiers, as the research questions related to understanding FSCR in Australian financial institutions rather than in any particular institution with limited generalisability. To this end, all the case data would be aggregated into a combined generic case based on the data from the three institutional cases. Further, the nature of the institutional cases is such that they are from the same industry sector rather than from different sectors. Also, all the participants have roles related to the management of organisational risk. A multi-case study design comprising three financial institutional cases was then stratified with three participants each to make a sample of nine participants; this was thought to be a reasonable
sample size to allow for retention of the benefits of a case study design (Eisenhardt 1991). It also provides a design benefit from the ability to cross-case triangulate and aggregate participant information providing for replicability across cases that gives increased generalisability over a single case (Patton 1999; Yin 2014). In addition, data volume is balanced with complexity to both provide an in-depth analysis typical of qualitative case methods and the facility to suggest generalisability beyond a single instance. These features of the design of the sampling aim to provide a foundation to make valid observations about Australian financial institutions without the loss of depth inherent in larger samples using quantitative methods (Dubois & Araujo 2007); this was the reason why three participants from each of three financial institutional cases were selected.

The multi-case sampling design above is based on a case replication logic rather than statistical logic. The latter is where the sample cases are randomly selected from the population of all 147 authorised deposit-taking institutions (APRA 2018) in Australia with equal probability, but with a large sample size to allow for statistical inferences to be made from standardised measures that lack depth. In contrast, replication logic concerns similar cases where similar depth data are expected to support generalisability but without the vulnerability of data distortion risk of a single case. In this multi-case study, based on replication logic, a chain referring sampling method (Alvi 2016) was used, geographically based in Melbourne, Australia. This is where the sample was selected non-probabilistically through referral initiated through both an industry network and through an institutional network following contact with the more senior participants.

The advantage of these case and participant selection methods is that they are also more suited to participants where there is some time and effort commitment required as a part of
participation (e.g., repeated interviews over time to develop in-depth data rather than short-term single instance interviews or a single questionnaire). Chain referring sampling methods (Alvi 2016) are also useful when the participants may be otherwise hard to reach or are few in number because of the specialised nature of their work.

Of the 147 deposit-taking institutions in Australia (APRA 2018) approximately 80% of capitalisation is held by the Tier 1 large banks, with Tier 2 medium sized and Tier 3 smaller banks holding the balance (APRA 2018). Three Australian owned financial institutions, one from each deposit-taking institutional capitalisation tier (large, medium and small), were selection for inclusion in this research. The selected banks subsequently invited the researcher to conduct interviews at the institution premises. An overview of the three banks are described next.

3.4.1.1 Bank X

The large Tier 1 Bank X is an international financial services organisation that provides a comprehensive range of financial products and services. Bank X is structured according to banking and wealth management operations, with international capital markets and an institutional banking business that operates in several global geographic regions.

Key businesses within Australia include personal banking, business banking, wholesale banking and wealth management, as well as group business services. The Bank X employs over 30,000 full-time equivalent employees and has over A$500 billion total assets; Bank X Retail includes over 500 branches and Bank X includes over 2,000 ATMs.

3.4.1.2 Bank Y

The medium sized Tier 2 Bank Y, an Australian-owned ASX listed company, has more than 80,000 shareholders; over 5,000 employees serve about 1.5 million customers in more than
500 communities Australia-wide. Assets are valued at more than $60 billion and market capitalisation at around $5 billion.

3.4.1.3 Bank Z
The small Tier 3 Bank Z employs over 500 full-time equivalent employees and has over $4000 million total assets.

3.4.1.4 Sample selection
The nine participants in the sample comprised three senior risk management professionals from each of the three financial institution cases selected. Senior risk managers were selected as they provided the point of contact between the researcher and the organisation. The risk managers were authoritative in relation to issues of risk and current risk management practices as they pertained to multiple organisation functions and divisional areas. They were selected following initial contact with the bank’s senior management by the researcher. This contact was made either through industry contacts or referral recommendations by industry contacts. The initial interviews revealed that the participants were keen to share knowledge on FSCR issues. Table 3.2 shows the participants’ characteristics, including institutional location, role, years of experience, education level and gender.

In each of the banks in the sample, bank board members sit on a risk management and compliance oversight committee. By and large, this committee oversees organisational performance on a number of risk-associated matters such as credit quality, risk related to the regulatory environment, monitoring risk appetite appropriateness and other perceived risks, such as sustainability. The more senior participants’ role-related activities variously involve ensuring the provision of risk-related information, which forms part of the periodic organisational risk report to the risk committee and subordinate committees within the
organisation. Participants 1, 5 and 7, being in more senior risk manager roles and delivering a wider span of the organisational division’s risk reporting responsibilities, ensure risk report information is routinely collected, centralised and reported to various divisional or functional area risk committees or councils, and may effectively be reported to the board-level risk committee. The organisational location of these senior risk roles tends to be in corporate divisions with a whole-of-institution focus on reputation, governance and corporate affairs. They may also have a cross-functional influencing or leadership role to support the disparate risk-related staff located in other divisions and geographies.

The remaining participants’ (2, 3, 5, 6, 8 & 9) roles tend to have narrower and a more operational scope of focus in their risk-associated roles. The location of their roles may be either in a corporate division or business unit based, but all have a focus on specific operational areas of risk such as audit, liquidity, business banking, products and markets, wealth finance, group development, financial crime, workplace performance or enterprise services and technology. Further, in addition to routine reporting, their roles involve a discrete risk issue investigation and analysis function as a response to discrete risk effects as they arise. Their role investigates what occurred and makes recommendations for remedial action in relation to the specific risk effect.

3.4.3 Interview protocol

The semi-structured interview schedule, shown in Appendix A, is described in the next section. The following interview protocol (adapted from Yin 2014) was followed before, during and after the interviews:
Table 3.2 Description of participants

<table>
<thead>
<tr>
<th>Participant Number</th>
<th>Financial Institution</th>
<th>Participant Role</th>
<th>Years of Experience</th>
<th>Education Level</th>
<th>Gender</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bank X</td>
<td>Senior risk manager</td>
<td>13</td>
<td>Bachelor</td>
<td>M</td>
<td>Tier 1</td>
</tr>
<tr>
<td>2</td>
<td>Bank X</td>
<td>Senior risk analyst</td>
<td>10</td>
<td>Master</td>
<td>M</td>
<td>Tier 1</td>
</tr>
<tr>
<td>3</td>
<td>Bank X</td>
<td>Senior risk consultant</td>
<td>15</td>
<td>Diploma</td>
<td>M</td>
<td>Tier 1</td>
</tr>
<tr>
<td>4</td>
<td>Bank Y</td>
<td>Senior risk analyst</td>
<td>17</td>
<td>Master</td>
<td>F</td>
<td>Tier 2</td>
</tr>
<tr>
<td>5</td>
<td>Bank Y</td>
<td>Senior risk manager</td>
<td>13</td>
<td>Bachelor</td>
<td>F</td>
<td>Tier 2</td>
</tr>
<tr>
<td>6</td>
<td>Bank Y</td>
<td>Senior risk analyst</td>
<td>11</td>
<td>Bachelor</td>
<td>M</td>
<td>Tier 2</td>
</tr>
<tr>
<td>7</td>
<td>Bank Z</td>
<td>Chief risk officer</td>
<td>19</td>
<td>Master</td>
<td>F</td>
<td>Tier 3</td>
</tr>
<tr>
<td>8</td>
<td>Bank Z</td>
<td>General manager risk</td>
<td>21</td>
<td>Bachelor</td>
<td>F</td>
<td>Tier 3</td>
</tr>
<tr>
<td>9</td>
<td>Bank Z</td>
<td>Senior risk manager</td>
<td>11</td>
<td>Bachelor</td>
<td>M</td>
<td>Tier 3</td>
</tr>
</tbody>
</table>

Before the interview:

a. Greet the participant;

b. Introduce the researcher;

c. The researcher provides brief information about the research (e.g., CRT, questions);

d. Explain privacy laws and RMIT University ethical standards;
e. Invite the participant to sign the privacy document; and,

f. Researcher sends by email brief information, objectives and what the interview expects to achieve.

During the interview:

a. Welcome the participant;

b. The researcher confirms and checks that the privacy document previously provided is signed;

c. The researcher seeks participant approval to record the interview;

d. Researcher describes the objectives of the interview; and,

e. The interview takes place and feedback from the participant is requested and noted.

After the interview:

a. Phone calls or send letters to thank the participant; and,

b. Review and create a transcript of the interview.
3.4.4 Interview procedures and schedule

The researcher collected the contact information of each participant from each of the respective financial institutions. During the phone discussion, the researcher invited the participant to take part in a group interview at RMIT University—some of the participants accepted the invitation, while others invited the researcher to visit the premises of their financial institution. Two participants confirmed that they would attend the RMIT University interview, while six confirmed that they would have the interview at their office. One interview was conducted through video conferencing. Interviews comprised a combination of individual interviews and group interviews. Three group interviews, one for each financial institution, were held as part of the reflecting back validation and included each of the three participants of the respective institutions. Most interviews had a duration of approximately 45 minutes.

The use of the telephone as a medium of data collection in this study was essential, because most of the participants involved were geographically dispersed across Australia and thus far from the researcher. Also, participants were re-contacted, with their consent, to reflect back the development of inquiry and to seek validation. The use of the telephone in qualitative data collection is endorsed by Cachia and Millward (2011, p. 266), who claimed that ‘this method provides good quality textual data on par with that obtained using face-to-face interview media, which can be examined using qualitative data analysis’. Together, with informal interviews, 15 formal, semi-structured in-depth telephone interviews were conducted with the participants between June and August 2016. Informal interviews were often used for clarification arising from previous interviews or to gain further insight through investigative inquiry. Formal interviews were digitally audio recorded, with consent obtained beforehand from the
participants. Further, handwritten notes were made during the interviews to complement the audio recording.

Semi-structured interviews were employed to serve as primary sources of data. The advantage of this interview methodology is that it allows richer descriptions of the phenomena under investigation, so that sense can be made (McMillan & Schumacher 2001; Punch 1998), and it is suited to the TOC method of inquiry. Informed by the TOC TP methods, which are integrative and interactive in nature (Goldratt 1990; Kim, Mabin & Davies 2008; Mabin & Balderstone 2003), semi-structured interview questions were utilised as part of the interviewing process. Based on the TP of TOC, the list of guiding questions shown in the semi-structured interview schedule (see Appendix A) was flexible and ‘not a tightly structured set of questions to be asked verbatim as written ... it is a list of things to be sure to ask about when talking to the person being interviewed’ (Lofland & Lofland 1995, p. 85). This enables considerable freedom for the interviewee in answering while, at the same time, focusing on the topics of the proposed study (Bryman 2004).

The semi-structured interviews comprised several steps and feedback, reflection and revision of the initial interview data through triangulation and validation. The semi-structured interview schedule comprising the guiding questions used in this process is shown in Appendix A. As the financial institution cases are large organisations, the interview inquiry process was broken into stages, with each part of each organisation inquired about successively, to build to a view of the entire organisation. Research about enterprise risk suggests that organisations can be conceptually viewed from different levels, from a lower or an operational level to higher corporate or strategic levels (Bromiley et al. 2015). This kind of organisational segmentation was intended to give a guiding structure to the inquiry process, and was subsequently validated.
with the participants regarding a shared view of the financial institution’s organisational characteristics. With indicative guiding questions shown in Appendix A at each step, the semi-structured interview steps were:

1. Participant role description questions
2. Organisational characteristic questions
3. Organisational structure validation/triangulation
4. Current state inquiry (CRT TOC TP – What to change?)
   a. Organisation’s functional operational level UDE questions
   b. Organisation’s functional business strategy level UDE questions
   c. Organisation’s functional corporate strategy level UDE questions
5. Current state validation/triangulation
6. Future state inquiry (FRT TOC TP – How to remediate risk?)
   a. Organisation’s functional operational level UDE transformation questions
   b. Organisation’s functional business strategy level UDE transformation questions
   c. Organisation’s functional corporate strategy level UDE transformation questions
7. Future state validation/triangulation

Each participant was interviewed on several occasions, to generate data initially and to verify cross-participant and cross-institutional synthesis. A sample of the interview transcripts is shown in Appendix B. From the interview inquiries, an initial list of risks identified and reported by the participants were extracted, collated and classified (see Appendix C) from the interview data. The list from the interviews was further developed and diagrammatic representations (see Appendix D) were used in subsequent interviews to elicit participant
feedback on causes of risk as part of the TOP-TP process of inquiry, as described in the next section.

3.5 Interview inquiry and the research process

Based on the TOC TP approach described in Section 3.3, CRT and FRT techniques and methods were used to identify and map issues from the operations level to the corporate level of the financial institutions (see Appendix E). During this process, the CRT and FRT maps were intended to be modified and updated on the basis of the industry participant recommendations, academic literature alignment and industry reports (e.g., Australian Payments Network 2019; Australian Banking Association 2019; Commonwealth of Australia AUSTRAC 2019). In short, the CRT and FRT maps represent a diagrammatic depiction of the summary or end-point of aggregated information elicited throughout the interview inquiry with the participants. This process is illustrated in Figure 3.6 and compromises several stages. The conceptual model (see Figure 2.1) derived from the literature informed a guiding synthesis of what was known about financial supply chain risk factors that was conveyed by the researcher to the participants with the objectives of both minimising the gaps in theory specific to the literature that the participant data might reveal, and to provide prompts and a shared terminology about the risks discussed. For example, when a participant identified an issue, the researcher would check whether this aligned with descriptions from the literature and identify a shared terminology.

In the TP process for the development of the CRTs that depict the current state of the financial institutions, there were four stages in the research process (see Figure 3.6). The first stage comprised questions about the organisational structure of the financial institutions. This was to develop a generalised organisational structure model that would find consensus among the
participants, and provide the conceptual scaffolding with which to portray the organisational location of risk and UDEs, and act as an interview question prompt to systematically work through UDEs and risks in the financial institutions. The second stage comprised questions (see Appendix A) concerning the examination of the UDEs and risks at the operational level of the financial institution cases. The third stage also comprised questions (see Appendix A) about UDEs and risks, but at the business strategy level of the financial institution cases. Similarly, the fourth stage comprised the same questions but directed at the corporate strategy level of the financial institution cases.

This process was repeated for the TP on the desired future states (the FRT shown in Figure 3.6), except that having already established the organisational structure, the questions concerning the development of the FRT (see Appendix A) first inquired about the operational level risk remediation in the first stage, then the second stage examined business strategy level remediation, and in the third stage, corporate strategy level risk remediation was the subject of the interview inquiry.
Figure 3.6 Overview of the research process

**Literature Review & Conceptual Framework**

**Thinking Process (TP)**

Current Reality Tree (CRT) development process:
Current state interview stages:

- Stage 1: Organisational structure
- Stage 2: Operational level risks
- Stage 3: Business strategy level risks
- Stage 4: Corporate strategy level risks

**Guiding Synthesis**
- Literature & conceptual model
- Pilot interviews
- Informant reports

**CRT Validation**

**Thinking Process (TP)**

Future Reality Tree (FRT) development process:
Future state interview stages:

- Stage 1: Operational level risk remediation
- Stage 2: Business strategy level risk remediation
- Stage 3: Corporate strategy level risk remediation

**FRT Validation**

Identification of financial supply chain risk factors

Feedback, Reflection & Revision

CRT output becomes an input to FRT development
Following working through identification and examination of risk at each of these functional levels of the organisational structure that was agreed early in the interview process, Figure 3.6 shows that both the CRT and FRT findings were iteratively developed through reflecting back to the participants through an interactive validation interview and inquiry process. The diagrammatic representations of the aggregated inquiry findings were used as exhibits in the later stages of the interview process to validate and develop the findings. Appendices D and E show examples that were used in developing the CRT and FRT diagrammatic representations of the findings. Last, the participants also were asked to describe how the results of the FRT analysis might be implemented and translated into organisation change management strategies using language and strategic management concepts familiar to contemporary financial institutions in Australia.

3.5.1 Reliability and validity

With case study methods, interview data reliability and validity should be appraised. As this study used qualitative research methods, it is important to ensure high-quality data (Neuman 2014). With qualitative interview data, participants describe their own experiences and views within a context. These data are therefore subjective and a researcher cannot remove the participants’ views to collect quality data. Instead, the participants’ descriptions are required to assist researchers to make sense of the participants’ descriptions of their experiences in the real world. Within case study research, there are two main types of validity: external or concurrent validity and internal validity. Internal validity relates to the questioning of the findings or conclusions and whether they are correctly aligned to the experiences described. According to Trochim (2000), internal validity is only relevant to studies, such as this one, that try to establish causal relationships and is suited to studies that assess the effects of
interventions. On the other hand, external validity questions the degree to which findings are credible and can be generalised to other similar settings to that in which the study occurred.

Lincoln and Guba (1985), Kvale (1996) and Neuman (2014) suggested a number of validity improvement techniques. One is prolonged engagement, which involves taking the time to understand the context of the participants, to assess the presence of misinformation and to establish trust. In this study, the researcher developed a collaborative relationship with the nine participants through multiple contacts both in person and by phone over an extended period of time. It was during these sessions that the researcher and participants were able to have conversations about their roles, their organisational cultures and so on, to assist the researcher to gain an understanding of the commonalities and differences among the three banking organisations. This was facilitated through synthesis of information about risks and other organisational characteristics across multiple participants and multiple cases.

More formal interviews were conducted at a time that was suitable for the participants, and in a familiar environment, typically their offices, where the locations were chosen by the participants. This made the participants feel comfortable and encouraged them to discuss their risk management role in the context of financial institutions.

According to Neuman (2014), validity can be improved through the use of participant checks; a process whereby the data collected by the researcher are validated against the participants’ understanding of the phenomenon being investigated. These validation interviews ensure that participants can reflect on the synthesis of information collated by the researcher from the other participants so as to develop a consensus description or view of the phenomenon under investigation through both validating and integrating procedures using an iterative feedback, reflection and adaption process with the participants.
Within the context of this study, there were multiple iterations of initial information elicitation, followed by reflecting back validation, and again followed by the researchers’ development of a consensus view of the information cross-validated with all participants, with some moderation in terminologies through reflecting back participant shared understandings and experiences as well as the researcher’s input from the synthesis of the literature. In so doing, any initial perceived differences between the participants were resolved by iteratively developing a shared view of a generic financial institution perspective. The intent was to develop, on each topic area covered, a generic consensus view using common terminology, but for which all the participants agreed reflected the shared meaning sitting behind whatever words they may have used initially through triangulation (Patton 1999; Yin 2014).

Reliability refers to whether the data are internally or externally consistent (Kvale 1996; Neuman 2014). Internal consistency questioned if the data provided were plausible, eliminated deception and ensured that the descriptions about organisational risk characteristics made sense. Through the observations and views of participants, the researcher believed that an accurate account was provided by all participants as they were all able to provide similar accounts of risk issues despite being located in different banks and in different roles, albeit all related to risk management. By the time the researcher had interviewed the final participant, the researcher was able to describe and depict financial institution risk characteristics, because of the consistency of information provided by the participants involved in this study.

External consistency refers to the ability to crosscheck the information provided by participants interviewed against each other through the use of triangulated data from different sources (Kvale 1996; Neuman 2014). In this study, the multi-case study design, comprising three banks of varying sizes and three participants from each bank, aimed to increase the likelihood of the
validity and generalisability of the findings to other banks and other types of financial institutions. This multi-case and multiple participant approach increased the triangulation of the data, ensuring that the information provided by the participants interviewed was accurate, and in turn, minimising the effects of individual distortion through misinformation, evasions, lies and fronts (Kvale 1996; Neuman 2014). Further, the participants drew on industry and internal papers in their operational industry views on risk (e.g., Australian Payments Network 2019; Australian Banking Association 2019; Commonwealth of Australia AUSTRAC 2019).

3.5.2 Ethical and critical reflections

Regarding the pre- and post-interviewing experiences of the researcher, the interviewing process was generally conducted smoothly. On receiving the necessary approval from the Ethics Committee, the researcher started engaging lists of participants and sending out invitation letters by mail. Once confirmation was obtained, an interview date and time were allocated, at each participant’s convenience. The interviewing process began with the participant being provided with the study consent form, to ensure voluntary participation. Further, all participants were given a guarantee that their identity would not be revealed and valuable information gained would be treated as confidential.

Approval from RMIT University Ethics Committee was obtained (RMIT Project Number 19204), and this study was classified as a low-risk study project (see Appendix F). In addition, certain procedures were undertaken to ensure overall study integrity. First, all participants were provided with a plain language statement of the overview of the study project and their rights as a participant (see Appendix G). Second, an informed consent form was provided prior to the interviewing process to ensure voluntary participation (see Appendix G). Finally, all nine participants agreed to be audio recorded. The participants were also assured that the data
collected would not be used for other purposes and their identities would not be disclosed. All recorded audio from the interviews are to be kept in a secure location for a period of five years.

3.6 Summary

This chapter provided an account of the study design and the approaches taken for data collection. The nature and purpose of the study have been explained in accordance with the chosen paradigm. Sample cases, the analysis approach and the organisations involved were described. The data collection techniques and method of analysis have been defined on the basis of the relevant protocols. The researcher’s position in relation to the philosophy underpinning this study was described. Next, Chapters 4 and 5 describe the findings of the analyses and present a participant validated aggregation of the data from the three institutional cases.
CHAPTER 4

ANALYSIS AND RESULTS:
CURRENT STATE ANALYSIS

4.1 Introduction

This chapter describes the findings of the application of the TOC TP approach comprising the construction of CRT. These depict what the application of the TOC TP methods to the case study data show as the current state of the underlying causes of the risks facing the participating financial institutions. The CRT method was applied to identify and portray the nature of financial institution risk. As described in Section 3.3.3.3, CRT comprises an iterative method of interactive inquiry where the participant semi-structured interview questions (Appendix A) aimed to reveal underlying causes, which were subsequently mapped to illustrate causal pathways.

The financial institution core risk effects or activities were identified by the participants (see Appendix C), which resulted from a failure to control the risk effects (see Appendices D and E). Specific functional areas contribute to various risks, such as card failures, which are business unit specific; other risks that are cross-organisational and not linked to particular business units were also identified by the participants. These risks were then aligned and arranged according to understanding their contribution and pathways regarding failing to meet or constraining attainment of the service objectives of the financial institution.

The CRT method of inquiry was applied to the aggregated participant interview data (see Appendix A) from nine senior risk management participants from three participating financial
institutions in three phases of analysis. First, to provide an organisational context for the presentation of the analysis, Section 4.2 describes the nature of the organisational functions and structures regarding what the participants thought was typical of financial institutions in Australia. The purpose of this was to provide a conceptual scaffolding with which to contextualise the CRT findings to the ecology of the financial institutions. Section 4.3 describes the findings of the CRT TP method mapped to the organisational structures described in Section 4.2. The CRT describes the contributions to risk and the proposed causal pathways among the risk-contributing characteristics at each organisational level.

4.2 Financial institutions in Australia

The case study financial institutions described in Section 3.4.1 were selected from each of three capitalisation tiers comprising large, medium and small. As a result, the sample of cases is thought to be broadly representative of financial institutions in Australia that include banking as part of their service offerings. From the participant interviews, the participating banks, despite capitalisation size differences, were confirmed to offer similar kinds of products and services, including transaction processing, payment risk management and liquidity in working capital finance. The institutions also offered advisory services to clients, for example, to navigate international payment methods for export and import risk management and ensure cost-effective financing.

An organisational structure shows how responsibilities for undertaking activities are directed through divisional business units or their equivalents towards the achievement of organisational objectives. An organisational structure is the perspective through which an organisation views its internal environment. Based on participant interviews with the senior risk management leaders from each of the three bank cases, a conceptual depiction of a
generalised financial institution functional structure was developed in the first stage of the research process (see Figure 3.6), from the questions from the second and third participant interview steps shown in Appendix A. As described in Section 3.4.4, the semi-structured interviews that preceded the application of CRT methods asked participants about the main divisions or business areas of their organisations. They were asked to adjust and validate drafts of an organisational structure that would be generally applicable to the financial institution cases. This comprises the main business divisions and the business units generally located within the divisions. It was agreed with the participants that this would be a consensus developed representation of generalised banking services. In response to questions about the validity of the structure developed, Participant 1 commented that despite the different tier sizes of deposit-taking institutions in Australia, the structure and functions ‘are often very similar, in my experience of the sector, despite volume differences in retail or wholesale banking, or the range or mixture of other financial products offered’. Figure 4.1 shows the generalised representation of the financial institution organisational structure developed with the participants and generally applicable to each of the case studies. The specific organisational structure charts internal to each of the three institutional cases were commercial-in-confidence and not able to be reproduced. However, the generalised depiction shown in Figure 4.1 was thought suitable for public domain research purposes by the participants.
Figure 4.1 Generalised financial institution structure
The institutional structure provides a point of reference for the interviews about risk and offers a staged approach to the participant inquiries building successively from each functional level and business area to develop a view of the entire institution. The institutional structure also describes how the case study data from the interviews on risk would be organised and portrayed in the CRT depictions. As shown in Figure 4.1, the financial institutional structure was validated as generally comprising three functional levels: the operations level, the business strategy level and the corporate strategy level. These are described in the next sections.

4.2.1 Operations level

The operations level of the financial institution shown in Figure 4.1. The functions are consistent with those described by Handfield (2013) in consideration of enterprise level consideration of risk where operational risks are distinguished from strategy risks. The operations level comprises those business operations that interface with both retail and business customers. It includes retail banking including customer-facing ATMs, internet banking and bank branch services. It also includes wholesale and business-to-business banking, financial products and marketing, and frontline operational technology services. Across all these business areas, it was agreed with participants to include people-centred services, external service provider management, regulatory compliance and technology functions.

4.2.2 Business strategy level

The business strategy level includes the organisational functions of business decision-making, operational strategy formulation and guidance for implementation into operations. This level provides the strategies that guide and shape the characteristics of retail operations, business
and wholesale banking business operations and enabling technology services. Figure 4.1 shows how business strategy units are aligned to divisional structures and guide banking operations. The business units at this level include the backroom functions that drive operational policies and sit behind the frontline, and customer-facing services that are located at the operational level.

4.2.3 Corporate strategy level

The corporate level functions shown in Figure 4.1 focus on corporate vision and mission, and provides for medium-to-longer-term strategic guidance of the organisation. The function of this level is to shape the nature and formulation of business strategy and the business as a whole. It takes account of environmental threats and opportunities, with the goal of maximising achievement of the corporate vision or mission. The corporate strategy level sets the policies that govern the organisation as a whole, and represents the organisation externally by ensuring policies are aligned with the requirements of the regulatory environment.

The corporate strategy covers four main areas, including the consumer businesses (aligned with retail banking), corporate, small and medium business customers (aligned to business banking), product and market business functions (aligned with the wholesale business), and enterprise services guiding all technology-related functions. Figure 4.1 shows how these corporate level functions are aligned and guide banking organisational divisions and business units.

In summary, according to the participants, from the questions shown in Appendix A, Figure 4.1 is the cumulative outcome of the stage of the interview inquiries regarding organisational characteristics and represents a consensus view developed with the participants. According to
the participants, this representation of structural and functional organisation is generally
typical of most banking and financial institutions operating in Australia. For example, in
response to the validation interview inquiry stage questions on organisational characteristics,
Participant 7 reported of the organisational structure representation:

\[
\text{It might vary in the very specific details and in the names given to a function in a}
\]
\[
\text{particular organisation, but overall it is a reasonable representation of the}
\]
\[
\text{generalised structure of Australian banks.}
\]

In the next section, detailed CRTs, which were iteratively developed with the participants, are
presented and described (see Section 3.5 and Figure 3.6 for a description of the participant
inquiry process). The CRT maps the dynamic relationships that occur between core risk
effects, and the financial institution functions and structures. This provides a basis for making
sense of the nature of risk causality in large and complex financial institutions.

4.3 Current state analysis

This section describes the results of the CRT method that was applied to identify and portray
the current state of the nature of financial institution risk developed with the participants. To
show the organisational location and dynamics of the risk attributes, the CRTs are organised
according to the functional structure characteristics described in Section 4.1, comprising an
operations level (Stage 2 of the research process shown in Figure 3.6), business strategy level
(Stage 3 of the research process shown in Figure 3.6) and corporate strategy level (Stage 4 of
the research process shown in Figure 3.6). Figure 4.1 provides the context for the detailed CRT
results that are described below and in Sections 4.3.1–4.3.5
The CRT method described in Section 3.3.3.3 was developed with questions from a participant interview inquiry process (Appendix A) that was iterative and interactive in nature (see Figure 3.6), where the purpose was to reveal the causes and effects of UDEs that affect the attainment of organisational objectives. Following the development of a participant consensus view of generalised organisational structure described in Section 4.2, the interview process inquired successively about the causes and effects of UDEs occurring at three stages, representing each of the institutional functional levels (the operations level, the business strategy level and the corporate strategy level). This was repeated for each of the four main UDE types aligned with each major financial institution divisions (see Figure 4.1). Appendix C shows an example of the list of risk effects derived and classified from the interview data. Appendix D shows a diagrammatic representation of these data summarised and aligned with the business units that were used as a prompt at subsequent participant interviews. The diagrammatic representations were used in the participant inquiry process to elicit dynamic risk effect cause-and-effect relationships from the participants. Appendix E shows the initial risk process map derived from Appendix D participant provided information, which was used in further interviews to finally develop and then validate the CRTs shown in Figures 4.2–4.7. The interview process (see Section 3.3.3.3) identified, examined and interrogated to reveal a shared view of the root causes behind the major sources and nature of the risks facing the financial institutions, taking account of the entire organisational context.

For ease of understanding, the CRT analysis is divided into four subtrees representing each of the four main organisational business functions corresponding to divisional organisational structures (see Figure 4.1). First, the area of demand-related risk where retail banking fails to meet customer needs is described in Section 4.3.1. Second, Section 4.3.2 describes the supply operations related risk area where banking fails to meet business-to-business targets. Third,
Section 4.3.3 describes product management failure, and Section 4.3.4 describes IT-related business disruption.

For each of these four business areas of the institutions, the four CRTs present the end result of the iterative and validated CRT development research process with the participants illustrated by Figure 3.6. The first part of the results description for each of the four CRTs (Sections 4.3.1–4.3.4) refers to the findings at the organisational operations level (see Section 4.2.1), followed by a description of findings at the business strategy level (see Section 4.2.2). Last, the four subtrees are combined into an entire institution CRT view in Section 4.3.5, including their interacting effects and the contribution of the corporate strategy level (see Section 4.2.3) to financial institution risk.

4.3.1 Current reality tree for demand in retail banking

This section discusses the reasons identified from inquiries with participants why retail banking fails to meet customer needs. The findings of the interview process are illustrated in Figure 4.2, which shows the retail banking CRT results. First, the validated participant observations in response to questions (see Appendix A) on the causes and effects of undesired risk effects occurring at the operational functional level of the organisation are described. Figure 4.2 shows that the core reasons why retail banking fails to meet customer needs (1.0) are hardware/software issues (coding, security, privacy) (1.4), limited capacity and capability of people-centred services (HR) (1.14) and limited adequate specification of policy and inflexible procedures (HR policy, operational procedures) (1.22). In response to questions (see Appendix A) about operational level UDEs, Participant 8 observed:
through this process I have become more aware that for each of the core reasons, they were manifested by several specific unwanted risks that were related to each other, when they are not always seen that way in practice.
Figure 4.2 Current reality tree for demand in retail banking

Business Strategy

Corporate Strategy

Decline in
consumer
business
performance
impacts business
and consumer
confidence(3.0)

Wholesale
business decline
fails to maximise
portfolio
outcomes (due to
product
costs)(3.3)

Small, medium and large business
departments underperforms and fails
to achieve shareholder targets(3.1)

Enterprise services
technology failure
because service is
under-developed and
technology risk is not
well managed
(disconnected from
enterprise)(3.4)

Extreme
disruption of
financial
payment
processes(3.
2)

Retail and small
business
disruption from
emerging
generations of
consumers
responding to
innovative new
businesses(2.10)

High credit risk
because borrowers fail
to make payments,
loss of principal and
interest, disruption to
cash flows and
increased collection
costs(2.12)

Underperformanc
e of digital and
direct growth in
the retail division
due to digital
disruption(2.11)

Negative consumer
credit retail and cobranded credit card
performance by
Australasian retail
credit
association(2.9)

Insurance and
superannuation
decline driven by
lower investment
yields(2.8)

Lack of
understanding of
retail
compliance
issues(2.0)

Financial market
decline as the result
of a major
catastrophic event,
financial crisis or
collapse of a longterm speculative
bubble(2.13)

Decline in
investment and
corporate
performance for
both debt and
equity(2.6)

Business fails
to handle
credit
operations
well(2.1)

Inaccurate balance
sheet and liquidity,
balance sheet
fluctuations, banks
manage the risks of
asset–liability
mismatch(2.5)

Enterprise Services
Technology Failure
because service is under
developed and
technology-risk is not
well managed
(disconnected from
enterprise )(3.5)

Customer service
levels and service
quality fail to meet
customer needs(2.14)

Enterprise
development declines
dues to decline in
screen and
assessment
platforms(2.7)
Customer service
satisfaction
decline(2.4)

Increasing complexity
makes it difficult to
integrate new fintech
with legacy
systems(2.3)

Poor business advice from staff, poor
culture in financial institutions and
their staff, audit-critical employees

(2.2)

No-cash
in the
ATM

(1.26)
Incorrect deposit
amount(1.25)

Limited policy
and inflexible
procedures (HR
policy,
operational
procedures)(1.22)

Insufficient continual
professional
development
(training, leadership,
communication)(1.21)

Non-fulfilment of
auditing requirements
and poor governance of
regulatory requirements
(APRA)(1.20)

Business monitoring
failure (evaluation)(1.19)

Operations

Customer transactions
failure(1.24)

Ineffective policy
and
governance(1.13)

Limited capacity
and capability of
people centred
services
(HR)(1.14)

Ongoing retail
resource allocation
issues(1.15)

More unsatisfied
customers come to
branch(1.16)

Internal politics
creates problems
inside the
business(1.12)

Current retail capacity is
limited(1.9)
There is a tremendous pressure
on retail staff to process
customer needs(1.11)

Branch staff
with limited
capacity to
perform
work(1.10)

Limited resources
(staff numbers,
equipment,
physical
space)(1.2)

Customers asked to
complete their
banking using the
online system(1.8)

Retail facilities
overcrowded (many
customers going to
branch)(1.18)

Poor recruitment process
puts pressure on business
(1.23)

Human data entry processing
error(1.17)

EFP machine
breakdown
(system support
failure, limited
cash
delivery)(1.6)

Phone banking
takes a long time to
be activated(1.7)

Online Banking unable to
support customer (the
online website has limited
resources )(1.3)

Hardware/
software issues
(coding, security,
privacy)(1.4)

Inadequate staff training
and induction(1.1)

Demand/Retail
banking fails to
meet customer
needs (1.0)

121

The number of
ATM technicians is
limited –
malfunctions &
ATM failure(1.5)


Hardware/software issues (1.4) arise from EFP machine breakdown (system support failure, limited cash delivery) (1.6), the limited number of technicians to cope with ATM malfunction (1.5) resulting in customer transaction failures (1.24), lack of ATM cash (1.26) and transaction errors such as incorrect deposit amounts (1.25). These technology disruptions result in online (1.3, 1.8) and phone banking (1.7) service failures and data processing errors (1.17). The flow-on effects of these electronic service failures lead to increased customer visits to branches (1.18), where the institutions are not adequately prepared for dealing with the consequences arising from the technology disruptions. In the branches, retail capacity is limited (1.9) and there is increased pressure on staff to process customer needs (1.11). Combined with limited resources (1.3), and magnified by internal political problems (1.12) and ineffective policies and governance (1.13, 1.22), these serve to compound the issues and the system copes poorly with disruptions to operational service delivery. This shows that risks from one set of effects move through the system, elevating and creating risk in functionally connected areas. Participant 3 observed that the risk movement ‘is like a snow ball picking up momentum and increasing in size as it rolls along’.

The operational level issues of limited capacity (1.10), lack of training preparation (1.21) and poor recruitment (1.23) are further compounded by inadequate staff training and induction (1.1), which, when combined with the limited capacity and capability of HR (1.14), creates limited policy and procedures (1.22). The combination of these undesired/risk effects contributes to poor fulfilment of regulatory requirements (1.20) and resource allocation issues (1.15). The ongoing limited capacity and capability of HR (1.14) also results from a failure of adequate business monitoring and evaluation (1.19), which also fails to detect, respond and remediate the other interacting effects described above (1.4, 1.9, 1.18, 1.22).
The demand in retail banking CRT (see Figure 4.2) shows that failing to meet customer needs is multidetermined by a complex interacting system of causes, most of which are interrelated and can be both determinants and effects, and which, in turn, can have other effects. For example, Participant 5 reported that:

*One of the problems that you've got in major financial institutions is people in divisions like IT don't see a full vantage of it. That's the operating effect that's occurring within the value chain, if you like, because one of the problems that you've got, for example, usually ATM failure. You may have been able to avert that if you had sufficient capacity to apply controls over that to actually identify the problem earlier or even before it occurred. The actual underpinning cause was not having a control, but the reason why it didn't have a control over it was I didn't have enough capacity in my HR to build a control.*

Other contributing operations level issues compounding retail banking failing to meet customer needs include non-fulfilment of auditing requirements and poor governance of regulatory requirements (APRA) (1.20), insufficient continual professional development (training, leadership, communication) (1.21), limited policy and inflexible procedures (HR policy, operational procedures) (1.22) and business monitoring and evaluation failure (1.19). The chain of interacting effects results in UDEs, contributing to why retail banking fails to meet customer need. Next, aggregated participant observations in response to inquiry (see Appendix A) about the causes and effects of undesired risk effects occurring at the business strategy level of the organisation are described.

The operational level risks, comprising limited policies (1.22), insufficient professional development (1.21), poor governance of regulatory requirements (1.20) and business
monitoring failures (1.19), all contribute to business strategy level failures, including a lack of strategic management understanding of retail compliance issues (2.0), poor handling of credit operations (2.1) and poor organisational culture factors such as poor business advice and audit critical employee attitudes (2.2). Lack of strategic management understanding of retail compliance issues (2.0) contributes to negative consumer credit retail and co-branded credit card performance by Australasian retail credit associations (2.9), which, in turn, contributes to retail and small business disruption from emerging generations of consumers responding to innovative new businesses (2.10), together with the underperformance of digital and direct growth in the retail division due to digital disruption (2.11). Poor organisational culture (2.2) contributes to a decline in investment and corporate performance for both debt and equity (2.6), insurance and superannuation declines are driven by lower investment yields (2.8), as well as negative feedback from inaccurate balance sheets and liquidity, and balance sheet fluctuations, such that banks must manage the risks of asset–liability mismatches (2.5). These, in turn, are influenced by an environment where there are high credit risks because borrowers fail to make payments, combined with the loss of principal and interest, disruption to cash flows and increased collection costs (2.12). Also affected are potential financial market declines because of major effects with negative effects (2.13). Declines in customer service satisfaction (2.4) arise from a range of customer-facing operational failures (1.4, 1.6, 1.24, 1.26), and with no apparent or effectively implemented risk control to counter the decline, such as via operational improvements, lead to falling customer service quality (2.14). In commenting on the CRT findings illustrated in Figure 4.2, Participant 2 reported that risk to customer satisfaction is influenced by multiple factors:

The common denominator across credit risk, operational risk, all these types of risk, is the risk management framework that sits in its own bubble and that drives
issue management, change management, obligation adherence, compliance adherence, operational risk business environment, definition, and how I said what the most important thing is would be risk appetite settings at the very top. That framework should ideally drive all this interaction and provide input into process improvement after the fact.

Similarly, technology issues and their impacts (1.4, 1.5, 1.6, 1.25, 1.26, 1.27) also account for disruptions in service delivery across all areas of banking operations. A cause is that increasing complexity makes it difficult to integrate new financial technologies (fintech) with old legacy systems (2.3) and enterprise development declines due to decline in screen and assessment platforms (2.7). Also contributing to customer satisfaction decline (2.4) is technology-related failure to meet customer service levels, quality and needs (2.14). For example, Participant 2 reported:

The challenge is that banks historically have had large, big, monolithic, centrally run technology systems which are incredibly hard to maintain, incredibly hard to update large amounts of investment that require multiple years of delivery to do. That's not the customer's experience when they can get a new app in three seconds right now and if they don't like that app they'll go and try another one. So part of the challenge we're facing is that we have a business model that's based around having central, everyone access to the data and customers are used to providing their data to 25 different apps, but that each of those apps is something very unique, very specific, and very value adding for the customer, and that's the challenge we're facing.
In summary, Table 4.1 shows the main or underlying demand in retail core risk effects that the CRT (Figure 4.2) analysis found, which contribute to retail banking failing to meet customer needs (UDEs). The most influential types of core risks that contributed to this failure were people-centred failures in the retail platform, external service provider disruptions, retail policies and regulatory limitations, and retail technology hub failures. These were interpreted as the underlying or most influential types of risk in that they were the types of effects that were most commonly reported by most of the participants. Further, when mapped onto the CRT and validated with the participants, these risk types either tended to form a shared junction point through which a number of other risk effect pathways would flow or they had influence on a range of other effects as shown by the interconnectivity in the CRT (see Figure 4.2).

The main or underlying core risk effect types are a summary type or categorisation name for groups of related undesired risk effects. For example, all people-centred failure core risk effects comprise some aspect of people-centred functions such as failures in recruitment, training, people policies and HR procedures. All of these retail demand failure related issues, which occur at the operations functional level of financial institutions, are both causes and also reflect inadequacies at the business strategy level. The corporate strategy level contributing causes are discussed in Section 4.2.5. Supply operations risk and business strategy level risk features of business banking is discussed next.
Table 4.1 Contributing CRT elements to demand in retail banking core risk effects

<table>
<thead>
<tr>
<th>Core risk domain</th>
<th>Retail demand core risk effects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core problem</td>
<td>Retail banking fails to meet customer needs</td>
</tr>
<tr>
<td>Main underlying core risk effect types (UDEs)</td>
<td>People-centred (HR) failures in the retail platform</td>
</tr>
<tr>
<td>Risk effects (UDEs)</td>
<td>External service provider disruptions</td>
</tr>
<tr>
<td></td>
<td>Retail policies and regulatory limitations</td>
</tr>
<tr>
<td></td>
<td>Retail technology hub failure</td>
</tr>
<tr>
<td>Inadequate staff training (e.g., recruitment process, inductions)</td>
<td>Outsourcing issues</td>
</tr>
<tr>
<td>Unfulfilled audit requirements (e.g., complaints)</td>
<td>Business support disruptions</td>
</tr>
<tr>
<td>Limited HR processes &amp; policies</td>
<td>Limited professional development and experience</td>
</tr>
<tr>
<td>Human error in database entries</td>
<td>Auditing issues (e.g., regulatory compliance)</td>
</tr>
<tr>
<td>IT system disruptions</td>
<td>Cyber security threats</td>
</tr>
<tr>
<td>Cyber security threats</td>
<td>EFTPOS &amp; ATM outages</td>
</tr>
</tbody>
</table>

4.3.2 Current reality tree for supply in business banking

This section describes the results of the CRT method applied to identify the reasons why participants thought business banking failed to meet business-to-business targets (see Figure 4.3). The validated participant observations in response to questions (see Appendix A) about undesired risk effects occurring at the operational functional level of the organisation are first described, followed by a description of risk effects at the business strategy level of the organisational structure. Figure 4.3 shows the core reasons for supply/business banking failures. These include various hardware or software issues (e.g., programming or phone and...
online banking disruptions) (1.2), limited capacity of people-centred services (HR) (1.14), and lack of operational policy guidance with an overreliance on inflexible procedures (1.17) unable to be adapted to meet situational needs including the adequate control of risks when they arise.

Hardware or software issues (1.2) contribute to a lack of adequate business monitoring and evaluation (1.20) and, together with the consequences of limited HR (1.14), contribute to online (1.1) and phone banking (1.5) issues and other technical failures (1.7) and lack of responding technicians (1.6). Failures in these areas cause more customers to both go online (1.4) and visit branches (1.8), placing pressure on limited retail capacity (1.3) and resources (1.13). All these issues contribute to internal political problems (1.15), which exacerbate ineffective policy and governance (1.16) and procedural policies (1.17), and contribute to lending operation discrepancies (1.22) and lack governance regarding the fulfilment of regulatory requirements (1.19). For example, Participant 1 reported:

*Certain issues which I can put down to lack of IT knowledge, which I can put as a supply chain system failure, which I can put in human errors and all that. I know the impacts to the business in terms of tests happen that we are approving loans by–there's a service agreement complement, like where the person can service that loan amount so an error is causing the customer's income to be calculated incorrectly which means you'll get a loan, even if you are not earning that much. So that's a major impact and that's happening in some loans. Capacity and capability are what comes to mind. Where you've got here–staff capability–it's part of that and I do see it coming from supply issues. We're also talking about resources. Across our point of view, I see those are the main drivers for HR issues.*
Limited people-centred services (1.14) contribute to poor professional and leadership development (1.18), lack of flexible policies (1.17) and monitoring and evaluation failures (1.20), and have multiple effects on failing to meet business-to-business targets when combined with the effects of business customer-facing services above (1.3, 1.9, 1.10, 1.13). Technical and other capacities are also affected by poor recruitment (1.21).

Business-to-business operational technical financial capacities can also affect adequate understanding of fluctuations in commodity and shares prices as well as interest rate issues (1.11), and lead to value at risk (VAR) (another company that adds features or services to an existing product, then resells it) miscalculations (1.12).

Next, the validated participant observations in response to inquiry (see Appendix A) about the causes and effects of undesired risk effects occurring at the business strategy level of the organisation are described. Operations level causes, non-fulfilment of auditing requirements and poor governance of regulatory requirements (APRA) (1.19), insufficient continual professional development (training, leadership, communication) (1.18), limited policy and inflexible procedures (HR policy, operational procedures) (1.17) and business monitoring and evaluation failure (1.20) contribute to business strategy level failures, including a lack of strategic management understanding of retail compliance issues (2.0), poor handling of credit operations (2.1) and poor organisational culture factors such as poor advice, lack of trust and behavioural issues (2.2).
Figure 4.3 Current reality tree for supply in business banking

- **Decline in consumer performance**
  - Limited policy and governance (HR, finance)
  - Customer service levels and service quality fail to meet customer needs (2.13)
  - Ineffective policy and governance (1.16)
  - Limited capacity and capability of people centred services (HR, finance) (1.14)
  - Internal policies and procedures out of line with business needs (1.15)
  - Insufficient training and professional development (HR, finance) (1.18)

- **Insufficient continual support for customers**
  - More unsatisfactory customers in the branch (1.10)
  - New customer service centres in the branch (1.9)
  - Customer service centres in the branch (1.8)

- **Retail and small business disruption from emerging generations of customers responding to innovative new businesses**
  - Underperformace of digital and direct growth in the retail division due to digital disruption (2.6)
  - Lack of understanding of retail compliance issues (2.0)
  - Negative consumer credit retail and co-branded credit card performance by Australasian retail credit association (2.3)
  - Insurance and superannuation decline driven by lower investment yields (2.5)

- **Business monitoring failure (evaluation)**
  - Non-fulfilment of auditing requirements and poor governance of regulatory requirements (APRA) (1.19)
  - Business fails to handle credit operations well (2.1)
  - Poor business advice from staff, poor culture, audit-critical employees (2.2)

- **High credit risk because borrowers fail to make payments, loss of principal and interest, disruption to cash flows and increased collection costs**
  - Fluctuation in commodity prices, share prices, interest rates (1.11)
  - Hardware/Software issues (coding, security, privacy) (1.2)
  - Mis-Calculation - VAR - None - VAR cause wrong evaluation (1.12)

- **Business monitoring failure (evaluation)**
  - Ineffective policy and governance (1.16)
  - Inaccurate balance sheet and liquidity, balance sheet fluctuations, banks manage the risks of asset-liability mismatch (2.14)
  - Inaccurate balance sheet and liquidity, balance sheet fluctuations, banks manage the risks of asset-liability mismatch (2.14)

- **Business monitoring failure (evaluation)**
  - Lack of understanding of retail compliance issues (2.0)
  - Internal politics creates problems inside the business (1.15)

- **Limited policy and inflexible procedures (HR policy, operational procedures)**
  - Limited policy and inflexible procedures (HR policy, operational procedures) (1.17)
  - Retail capacity is limited (1.3)
  - Ongoing retail resource allocation issues (1.13)
  - Supply/Business banking fails to meet business-to-business targets (1.0)

- **External politics and cultural changes outside the business**
  - Customer service levels and service quality fail to meet customer needs (2.13)
  - Enterprise development due to decline in economic and investment prospects (1.1)
  - Increasing complexity makes it difficult to integrate new fintech with legacy systems (2.11)

- **Supply/Business banking fails to meet business-to-business targets**
  - Non-fulfilment of auditing requirements and poor governance of regulatory requirements (APRA) (1.19)
  - Non-fulfilment of auditing requirements and poor governance of regulatory requirements (APRA) (1.19)
  - Corporate Strategy - Business Strategy - Operations

  - Customers asked to complete their banking using the online system (1.4)
  - More unsatisfied customers come to the branch (1.8)
  - Retail facilities overcrowded (many customers going to branch) (1.10)
  - Ineffective policy and governance (1.16)
  - Insufficient continual support for customers (1.15)

- **End-to-end performance issues across all business activities (1.20)**
  - Customers fail to fund accounts, process applications (1.2)
  - Customers wait a long time to receive funds (1.7)
  - ATM failure due to limited number of technicians (1.6)
  - EFP machine breakdown (system support failure, limited cash delivery) (1.7)

- **Supply/Business banking fails to meet business-to-business targets**
  - Non-fulfilment of auditing requirements and poor governance of regulatory requirements (APRA) (1.19)
  - Non-fulfilment of auditing requirements and poor governance of regulatory requirements (APRA) (1.19)
  - Corporate Strategy - Business Strategy - Operations

  - Customers asked to complete their banking using the online system (1.4)
  - More unsatisfied customers come to the branch (1.8)
  - Retail facilities overcrowded (many customers going to branch) (1.10)
  - Ineffective policy and governance (1.16)
  - Insufficient continual support for customers (1.15)
Lack of strategic management understanding of retail compliance issues (2.0) causes negative consumer credit retail and co-branded credit card performance (2.3) which, in turn, causes retail and small business disruption from emerging generations of consumers responding to innovative new businesses (2.4), together with the underperformance of digital and direct growth in the retail division with digital disruption (2.6). Poor handling of credit operations (2.1) also co-contributes to negative consumer credit (2.3) and business disruptions (2.6).

Poor organisational culture and advice (2.2) contribute to a decline in investment and corporate performance for both debt and equity (2.8) and insurance and superannuation declines driven by lower investment yields (2.5). Poor organisational culture and advice (2.2) also contributes to inaccurate balance sheets and liquidity, balance sheet fluctuations, and bank management of the risks of asset–liability mismatches (2.14). These, in turn, contribute to an environment where there are high credit risks because borrowers fail to make payments, combined with the loss of principal and interest, disruption to cash flows and increased collection costs (2.7). Also affected are potential financial market declines because of major effects with negative effects (2.9).

As described in the previous section, customer service satisfaction was identified as in decline (2.13), arising from a range of customer-facing operational failures, but with no apparent business strategy to counter the decline through operational improvements. Similarly, technology issues and their impacts (1.2, 1.6, 1.7, 1.22, 1.23, 1.24, 1.25) also account for disruptions in service delivery across all areas of banking operations. An effect is that increasing complexity makes it difficult to integrate new financial technologies (fintech) with old legacy systems (2.11) and enterprise development declines due to declines in screen and
assessment platforms (2.12). Also contributing to customer satisfaction decline (2.10) is technology-related failure to meet customer service levels, quality and needs (2.13).

Similar to retail issues, the business banking CRT shows that failing to meet business-to-business targets is multidetermined by a complex interacting system of causes, most of which are related and can operate as both determinants and effects, and which, in turn, have other effects. When supply in business banking failure occurs, customer needs are not met and overall banking service delivery underperforms. For example, Participant 2 observed:

*Technology, absolutely. We are increasingly reliant on outsourced or third-party providers. I'm interested in HR and the payments process. This is a consequence of that. We're saying there's also a driver there that relates to the impact that regulations and policies have on how the business can do—what activities they can do and how it can do them. On top of that, if the staff aren't trained well, then there will be errors leading to compliance risks and other impacts. Not enough people, capacity, capability—all those sorts of things related to people skills So it is a cultural issue and an HR issue. In operational risk, we talk about people, processes, and systems. You're aligned.*

In summary, Table 4.2 shows the main or underlying supply in business banking core risk effects that the CRT (Figure 4.3) analysis identified as contributing to business banking failing to meet business-to-business targets (the UDE). The most common types of core risks found that contributed to this failure in supply in business banking were people-centred failures in business operations, external service provider disruptions, policies and regulatory limitations, and technology hub failures. These are shown in the CRT (see Figure 4.3), where they form
junctions where multiple effect pathways pass through or are interconnected with multiple other effects.

All of these supply in business banking failures that occurred at the operations functional level are both causes and also reflect inadequacies at the business strategy level of the financial institutions. The corporate strategy level contributing causes and effects are discussed in Section 4.3.5. Product management failure is discussed next.

Table 4.2 Contributing CRT elements to supply in business banking core risk effects

<table>
<thead>
<tr>
<th>Core risk domain</th>
<th>Supply in business banking risk effects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core problem</td>
<td>Business banking fails to meet business-to-business targets</td>
</tr>
<tr>
<td>Main underlying core risk effect types (UDEs)</td>
<td></td>
</tr>
<tr>
<td>People-centred (HR) failures in business operations</td>
<td></td>
</tr>
<tr>
<td>External service provider disruptions</td>
<td></td>
</tr>
<tr>
<td>Policies and regulatory limitations</td>
<td></td>
</tr>
<tr>
<td>Technology hub failures</td>
<td></td>
</tr>
<tr>
<td>Risk effects (UDEs)</td>
<td></td>
</tr>
<tr>
<td>Poor recruitment process</td>
<td></td>
</tr>
<tr>
<td>Insufficient professional development</td>
<td></td>
</tr>
<tr>
<td>Limited HR processes &amp; policies</td>
<td></td>
</tr>
<tr>
<td>Frequent internal and external fraud</td>
<td></td>
</tr>
<tr>
<td>Outsourcing issues</td>
<td></td>
</tr>
<tr>
<td>Government interventions</td>
<td></td>
</tr>
<tr>
<td>Regulatory non-compliance (APRA)</td>
<td></td>
</tr>
<tr>
<td>System failures</td>
<td></td>
</tr>
<tr>
<td>Online banking outages</td>
<td></td>
</tr>
<tr>
<td>Business transaction disruptions</td>
<td></td>
</tr>
</tbody>
</table>
4.3.3 Current reality tree for product management

This section describes the findings of the CRT analysis for product management failure. First, the validated participant observations in response to questions (see Appendix A) about the causes and effects of undesired risk effects occurring at the operational functional level of the organisation are described. Such failure mostly occurs in wholesale banking, where funds are borrowed and lent between local and international banks, and with exchanges made at either dollar value or with an interest rate. Major external effects such as natural disasters, political upheaval and public ethical and legal issues all also have significant impacts on product management risk but are outside the scope of this research.

Routine or ongoing wholesale-related operational causes of product management failure are illustrated in Figure 4.4, which shows the core reasons given by the participants for product management failure. These include various hardware or software issues (e.g., programming or phone and online banking disruptions) (1.1), limited capacity of HR (1.15), and lack of operational policy guidance with an overreliance on inflexible operational procedures (1.16) unable to be adapted to meet situational needs. Participant 9 highlighted multiple factors affecting product risk:

A lot of the things that will hurt a product's success are not the things that the product manager thinks of at the very first instance. They will be things like the ability of the supply chain to actually meet the requirements of the products. So that's a live example of something going on at the moment. So, you think, we’ll base a product on XYZ, but if the vendor can't meet those timeframes, the cost of leaving them is carving into the benefit. There is innovation disruption happening in that space. There are compliance complexities to that which we are not mature enough
to manage so you've created a product which is beyond our compliance capabilities.

Hardware or software issues (1.1) contribute to a lack of adequate business monitoring and evaluation (1.12) and to limited people-centred services (1.15). Online (1.7, 1.9) and phone banking (1.8) issues and other technical failures (1.2, 1.19, 1.20, 1.21) are directly or indirectly caused by hardware or software issues (1.1). Failures in these areas cause more customers to go online (1.9) and visit branches (1.10, 1.11), placing pressure on limited resources (1.17). All these issues exacerbate inflexible procedures (1.16), poor professional and leadership development (1.14), and monitoring and evaluation failures (1.12), and have multiple effects. Technical and other capacities are also affected by poor recruitment (1.21). Product management failures collectively cause lending operation discrepancies (1.3).

Different product management effects exist for different products at financial institutions, with many problems originating from lending operational discrepancies (1.3). Financial institutions are subject to annual fluctuations in commodity pricing, shares and interest rates, while operational technical financial capacities can also affect adequate understanding of fluctuations in commodity and shares prices as well as interest rate issues (1.6), leading to VAR miscalculations (1.5). For example, Participant 9 reported that:

*In foreign currency options, part of the reason for the failures was that the managing office was under resourced, which in turn was because of human error and HR capacity and capability.*
Figure 4.4 Current reality tree for product management

- Decline in consumer business performance impacts business and consumer confidence.
- Online banking fails to support customers due to limited functionality.
- Hardware/software issues (e.g., security, performance).
- Human data entry processing errors.
- Phone banking fails to process requests.
- EFT/cheque processing errors.
- Customer service failure.

- Increased complexity makes it difficult to integrate new fintech with legacy systems.
- Hardware/software issues (coding, security, privacy).
- Mis-calculation or no VAR cause wrong evaluation.
- Incorrect deposit amount.
- Limited capacity and capability of people-centred services.
- On-line/branch transaction failures.
- No cash in the ATM.
- EFP machine breakdown.

- Customer satisfaction decline.
- Customer transactions failure.
- Corporate strategy.
  - Customers asked to complete their banking using the online system.
  - More unsatisfied customers come to the branch.
  - Retail facilities overcrowded (many customers going to branch).

- Business performance.
  - High-level risk because business and customers are not aligned.
  - Decline in investment and corporate performance for both debt and equity.
  - High credit risk because borrowers fail to make payments, loss of principal and interest, disruption to cash flows and increased collection costs.

- Financial market decline as the result of a major catastrophic event, financial crisis or collapse of a long-term speculative bubble.
- Failure of organizational structures and regulations due to inadequate controls within the business.

- Insufficient continual professional development (training, leadership, communication).
- Non-fulfilment of auditing requirements and poor governance of regulatory requirements (APRA).
- Retail and small business disruption from emerging generations of consumers responding to innovative new businesses.
- Limited policy and inflexible procedures (HR policy, operational procedures).

- Small, medium, and large business departmental understandings fail to achieve desirable outcomes.
- Financial payment processes fail to achieve desirable outcomes.
- Business monitoring failure (evaluation).

- Insufficient continual professional development.
- Poor recruitment process puts pressure on business.
- Retail and small business disruption: Revenue from emerging generations of consumers responding to innovative new businesses.
- Failure of organizational structures and regulations due to inadequate controls within the business.
- Limited policy and inflexible procedures.
- Product management failure.
Next, the validated and aggregated participant observations in response to inquiry (see Appendix A) about the causes and effects of undesired risk effects occurring at the business strategy level of the organisation are described. Operations level causes, non-fulfilment of auditing requirements and poor governance of regulatory requirements (APRA) (1.13), insufficient continual professional development (training, leadership, communication) (1.14), limited policy and inflexible procedures (HR policy, operational procedures) (1.16) and business monitoring and evaluation failure (1.12) were caused by a chain of effects from operational level UDEs. These UDEs (1.12, 1.13, 1.14, 1.16) contributed to business strategy failures, including a lack of strategic management understanding of retail compliance issues (2.0), poor handling of credit operations (2.1) and poor organisational culture factors such as poor advice, lack of trust and behavioural issues (2.2). In relation to product management disruptions, Participant 6 observed that:

"It could be any sort of process really, so it could be how we transfer funds between banks over ten years old. There's a written process around that and that will have a number of controls built into it, but the person executing that process, following it, could follow the process as it's written and if there are errors in the actual way that it's documented, you could still end up with a risk or an actual disruptive effect."

Lack of strategic management understanding of retail compliance issues (2.0) contributes to negative consumer credit retail and co-branded credit card performance by Australasian retail credit associations (2.13), which, in turn, contributes to retail and small business disruption from emerging generations of consumers responding to innovative new businesses (2.14), together with the underperformance of digital and direct growth in the retail division due to digital disruption (2.11). Poor handling of credit operations (2.1) is also a contributing factor.
Poor organisational culture and advice (2.2) causes a decline in investment and corporate performance for both debt and equity (2.7), and insurance and superannuation declines are driven by lower investment yields (2.12), contributing to an environment where there are high credit risks because borrowers fail to make payments, combined with the loss of principal and interest, disruption to cash flows and increased collection costs (2.10). Poor organisational culture and advice (2.2) also causes negative feedback from inaccurate balance sheets and liquidity, balance sheet fluctuations and how banks manage the risks of asset–liability mismatches (2.3), contributing to potential financial market declines because of major effects with negative effects (2.9). The influences of organisational culture were described by Participant 5, who stated that:

*In reference to culture, I have a saying that you can create the perfect mousetrap. It’s not an original saying, but if people won't use it, it's useless. So, I think your risk design, you're getting the full value chain, working together, owning responsibility. That comes down to your culture, so you've got to make sure that culturally that is seen as the preferred direction. You've got to make sure you don't build a pocket of resistance to the culture of the organisation.*

As described in previous sections, customer service satisfaction is in decline (2.4) arising from a range of customer-facing operational failures, but with no apparent business strategy to counter the decline, through either operational or business strategy improvements. Similarly, technology issues and their impacts (1.1, 1.2, 1.4, 1.19, 1.20, 1.21) also account for disruptions in service delivery across all areas of product management. A cause is that increasing complexity makes it difficult to integrate new financial technologies (fintech) with old legacy systems (2.5) and this contributes to enterprise development declines due to declines in screen
and assessment platforms (2.6). Also, there is a technology-related failure to meet customer service levels, quality and needs (2.8). Similar to other operational issues, the product management CRT shows that failure is multidetermined by a complex interacting system of causes, most of which are related and can be both determinants and effects, and which, in turn, have other effects.

In summary, Table 4.3 shows the main product management core risk effects found by the CRT (Figure 4.4) analysis as contributing to the product management failure UDE. The most common types of core risks that contributed were product- and market-centred failures, product and external service provider disruptions, product and market policy and regulatory limitations, and product and market technology hub failures. These are shown in the CRT (see Figure 4.4), where they form junctions where multiple effect pathways pass or are interconnected with multiple other effects.

The product management failure related issues described above, which occur at the operations and business strategy levels of the bank, are also due to inadequacies at the corporate strategy level. The corporate strategy level contributing causes are discussed in Section 4.3.5. IT failure is discussed next.

4.3.4 Current reality tree for information technology

This section describes the findings of the CRT analysis regarding the reasons why IT issues disrupt business operations. Technology is major contributor that enables financial institution performance. As described in the literature in Chapter 2 and validated by the participants, technology disruptions are major service enterprise risk factors for business operations. Figure 4.5 shows the CRT for IT business disruptions.
Table 4.3 Contributing CRT elements to product management core risk effects

<table>
<thead>
<tr>
<th>Core risk domain</th>
<th>Product management core risk effects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core problem</td>
<td>Product management failures</td>
</tr>
<tr>
<td><strong>Main underlying core risk effect types (UDEs)</strong></td>
<td><strong>Product and market failures</strong></td>
</tr>
<tr>
<td>Risk effects (UDEs)</td>
<td>Miscalculation of VAR</td>
</tr>
<tr>
<td></td>
<td>Human database processing error</td>
</tr>
</tbody>
</table>

First, the validated and aggregated participant observations in response to inquiry (see Appendix A) about the causes and effects of undesired risk effects occurring at the operational level of the organisation are described. Figure 4.5 shows that the core or underlying reasons why IT business disruptions occur (1.0) are hardware/software issues (coding, security, privacy) (1.1), limited capacity and capability of HR (1.14) and limited availability of policy guidance giving flexibility to adapt to situational specific circumstances and an overreliance on inflexible and invariant procedural specifications (HR policy, operational procedures) (1.15).
Hardware/software issues (1.1) cause electronic funds processing machine (ATM) breakdowns (system support failure, limited cash delivery) (1.2), and potentially exhaust the limited number of technicians to cope with ATM malfunction (1.22), resulting in customer transaction failures (1.19), lack of ATM cash (1.21) and transaction failures (1.20). These result in online (1.6, 1.7) and phone banking (1.9) flow-on effects, which also include increased customer visits to branches (1.8) where retail capacity is limited (1.13) and increased pressure on staff to process customer needs (1.12). Illustrating the importance of IT, Participant 5 recalled an incident where thousands of customers’ information was released due to an IT error:

*It has an impact on their reputation, bank reputation, and safety because the bank looks into the safety as well. The interesting factors that are starting to apply to my mind is with digital technology, the customer can probably, in most cases, see what your internal system can see. These layers of non-disclosed control are starting to become more and more blurred as the system starts to digitise themselves. What occurred in that situation was they sought to maximise their capital market value in the short term (instead of investment in IT risk controls) which is an unsustainable business model and because they were doing it via cost control, not carrying business efficiency with it as well, you effectually had a breakdown in controls and you had a calamity or multiple calamities.*

Financial institutions are subject to annual fluctuations in commodity pricing, shares and interest rates, where operational IT business disruptions can cause errors and miscalculations about fluctuations in commodity and share prices as well as interest rate issues (1.11) and also lead to VAR miscalculations (1.4).
Figure 4.5 Current reality tree for information technology
All these issues are compounded by the limited capacity and capability of HR (1.14), which contributes to limited policy and procedures (1.15), insufficient professional development (1.16) and the poor fulfilment of regulatory requirements (1.17). The ongoing limited capacity and capability of people-centred services (1.14), as well as IT failures and capacity to cope with disruptions, also result from failure of adequate business monitoring and evaluation (1.18).

Next, the aggregated and validated participant observations in response to inquiry (see Appendix A) about the causes and effects of undesired risk effects occurring at the business strategy level of the organisation are described. The operations level causes, non-fulfilment of auditing requirements and poor governance of regulatory requirements (APRA) (1.17), insufficient continual professional development (training, leadership, communication) (1.16), limited policy and inflexible procedures (HR policy, operational procedures) (1.15) and business monitoring and evaluation failure (1.18) are caused by many elements of a chain of effects arising from operational UDEs. In turn, these operational UDEs also cause business strategy failures, including a lack of strategic management understanding of retail compliance issues (2.0), poor handling of credit operations (2.1) and poor organisational culture factors such as poor advice and lack of trust (2.2).

Lack of strategic management understanding of retail compliance issues (2.0) contributes to negative consumer credit retail and co-branded credit card performance by Australasian retail credit associations (2.11), which, in turn, contributes to retail and small business disruption from emerging generations of consumers responding to innovative new businesses (2.12), together with the underperformance of digital and direct growth in the retail division due to digital disruption (2.13). Poor handling of credit operations (2.1) also contributes to these
issues. Participant 5 explained how lack of strategic management allowed person-centred and other risks to become uncontrolled:

*We have a whole host of third-party relationships which power the supply chain, but they haven’t been created in the most commercially sensible ways because it's a lack of contractual knowledge by either party or it's a lack of understanding the broader domain in which those contracts or relationships are formed.* So the contract formation follows having superior negotiation skills (person-centred) based on knowledge, education, understanding of the domain. Everything from a why did we lock in a three-year contract when we know that technology is changing, we should only go for a 12-month contract. The cost of production is x but we can see there's innovation overseas–gaps in our supply chains which relates to IT security. We need a fresh look at what's the state of the world more broadly and how rapidly things are changing.

Poor organisational culture (2.2) causes a decline in investment and corporate performance for both debt and equity (2.5) and insurance and superannuation declines are driven by lower investment yields (2.10), as well as negative feedback from inaccurate balance sheets and liquidity, and balance sheet fluctuations mean that banks must manage the risks of asset–liability mismatches (2.4). These, in turn, create an environment where there are high credit risks because borrowers fail to make payments, combined with the loss of principal and interest, disruption to cash flows and increased collection costs (2.9). Also affected are potential financial market declines because of major effects with negative effects (2.8).
As described in the previous sections, customer service satisfaction is in decline (2.3) arising from a range of customer-facing operational failures, but with no apparent business strategy to counter the quality decline (2.7).

Similarly, technology issues and their impacts (1.1, 1.2, 1.3, 1.5, 1.19, 1.20, 1.21) also account for disruptions in service delivery across all areas of banking operations. A compounding factor is that increasing complexity makes it difficult to integrate new financial technologies (fintech) with old legacy systems (2.14) and, as a result, enterprise development declines due to declines in screen and assessment platforms (2.6). Related to the customer satisfaction decline (2.3) is a technology-related failure to meet customer service levels, quality and needs (2.7).

The CRT (see Figure 4.5) shows that capacity to manage IT business disruption is multidetermined by a complex interacting system of causes most of which are related and can be both determinants and effects, and which, in turn, have other effects on all other parts of the financial institution. Table 4.4 summarises the most common IT-related core risk effects cited by the participants and that the CRT (Figure 4.5) shows as contributing to the IT disruptions UDE. In the CRT (see Figure 4.5), these main effects form junctions where multiple effect pathways pass or are interconnected with multiple other effects.

In summary, Table 4.4 shows the types of core risks that were interpreted as the most influential by the CRT analysis in terms of contributing to IT business disruptions. These were IT system people-centred failures, external service provider disruptions, policy and regulatory compliance limitations, and technology hub failures. Participant 9 illustrated the interconnection of IT as an enabler of the supply chain and how external service providers are important for IT risk:
We in the industry—tend to outsource without understanding enough about who owns the risk and what other, what other overheads do you need to actually manage the process well, but again, technology is the 50% enabler and support for managing risk in the supply chain because it, it’s the mechanism by which you manage your data and do the analysis to make better decisions. It's the transmissive conduit for sharing information and presenting information.

Table 4.4 Contributing CRT elements to IT core risk effects

<table>
<thead>
<tr>
<th>Core risk domain</th>
<th>Information technology core risk effects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core problem</td>
<td>IT business disruptions</td>
</tr>
<tr>
<td>Main underlying core risk effect types (UDEs)</td>
<td></td>
</tr>
<tr>
<td>IT system people-centred (HR) failures</td>
<td>External service provider disruptions</td>
</tr>
<tr>
<td>Lack of IT knowledge</td>
<td>Communications and technology breakdowns</td>
</tr>
<tr>
<td>Human database processing errors</td>
<td>Data security for Privacy Act concerns</td>
</tr>
<tr>
<td>EFTPOS machine breakdown</td>
<td></td>
</tr>
</tbody>
</table>

All of these IT business disruption related issues described above, which occurred at the operations and business levels of the bank, also reflect and cause inadequacies at the corporate strategy level. The corporate strategy level contributing causes are discussed in the next section.
4.3.5 A combined current reality tree for the entire organisation

In each of the previous four sections on the operational UDEs (demand in retail failing to meet customer needs (Section 4.3.1), supply in business banking failing to meet business-to-business targets (Section 4.3.2), product demand failure (Section 4.3.3) and IT business disruption (Section 4.3.4), the results of participant validated responses to questions (see Appendix A) about operations level and business level causes of UDEs were each described individually. In this section, the four CRTs are combined into a single CRT representing the whole of the organisation. In addition, how each of the four divisional business areas were thought by the participants to interact with corporate strategy level UDEs are described. Corporate strategy level UDEs are described in this whole-of-organisation section on CRT findings because the nature of the corporate strategy level is concerned with all parts of the financial institution as a whole, as all parts are intended to work together to collectively contribute to the achievement of strategic objectives and the financial institution mission.

Figure 4.6 shows the combined CRT for all four UDE areas previously described individually. Figure 4.6 is an aggregated version of the previous four current reality subtrees, with shared or common CRT elements combined. This gives a whole-of-organisation view of risk, whereas the subtrees in Sections 4.2.1–4.2.4 gave a business-type or divisional-specific view. Like the previous CRTs, this combined CRT was a consensus, validated with the participants.
There is a tremendous pressure on the retail staff to process customer needs. Ineffective policy and regulatory requirements lead to errors. Inadequate staff training creates problems. Internal politics and limited resources are major obstacles. Lack of adequate staff training and induction. Lack of adequate policy and procedures. Limited capacity and capability of people and equipment. Inflexible hardware/IT systems. Excessive projects. Figure 4.6 Combined current reality tree for the entire organisation.
This section also describes the findings from participant responses to inquiries about the causes of corporate strategy level UDEs. For example, the response of Participant 2 to questions (see Appendix A) about corporate strategy level UDEs illustrated how people-centred failure is a shared issue across all the business areas examined in the previous CRTs, as people-centred functions are located at multiple functional levels:

In our organisation, the responsibility for training exists with the business, not the HR area. So those failures or the drivers that relate to people. It’s people-centred failures, that would include error, lack of training, lack of capability. This is a pandemic that fuels multiple risks—all of those sort of things—not enough people, capacity, capability—all those sorts of things related to people skills.

The operational level causes of underlying UDEs are shown in Figure 4.6. These comprise limited policy and inflexible procedures (HR policy, operational procedures) (1.23), limited capacity and capability of people-centred services (1.3), and hardware and software issues (1.9). These resulted from many elements of the chain of effects, resulting in the main UDEs (1.0, 1.1, 1.2, 1.3). The core effects of these UDEs on the business strategy level included a lack of strategic management understanding of retail compliance issues (2.0), poor organisational culture factors such as poor advice and lack of trust (2.2), in-service balance fluctuations and mismatches (2.10), customer service satisfaction decline (2.11), and the impact of the complexity of fintech and legacy systems on back office banking processes (2.12).

Lack of strategic management understanding of retail compliance issues (2.0) caused negative consumer credit retail and co-branded credit card performance (2.3), which, in turn, caused
retail and small business disruption from emerging generations of consumers responding to innovative new businesses (2.4). Poor handling of credit operations (2.1) also contributed to underperformance of digital and direct growth in the retail division due to digital disruption (2.6).

Poor organisational culture (2.2) caused a decline in investment and corporate performance for both debt and equity (2.8), and insurance and superannuation declines are driven by lower investment yields (2.5), while negative feedback from inaccurate balance sheets and liquidity, and balance sheet fluctuations mean banks must manage the risks of asset–liability mismatches (2.10). These, in turn, create an environment where there are high credit risks because borrowers fail to make payments, combined with the loss of principal and interest, disruption to cash flows and increased collection costs (2.7). Also affected are potential financial market declines because of major effects with negative effects (2.9). As described in the previous individual business area CRTs in the four previous sections, customer service satisfaction has declined (2.11), arising from a range of customer-facing operational failures, combined with no apparent business strategy to counter the decline through operational improvements.

Similarly, technology issues and their impacts (1.9, 1.27, 1.32, 1.33, 1.34) also accounted for disruptions in service delivery across all areas of banking operations. Increasing complexity makes it difficult to integrate new financial technologies (fintech) with old legacy systems (2.12) and enterprise development declines due to declines in screening and assessment platforms (2.13). As customer satisfaction declines (2.11) from all these contributing causes, there is a flow-on effect from technology-related failure to meet customer service levels, quality and need (2.14).
Figure 4.6 shows that customer-facing operational failures (retail, wholesale, products and IT services), while having causes related to operational shortcomings, also compound various business strategy failures. These business strategy failures, in turn, contribute to corporate strategy shortcomings and reduce capability to meet organisational objectives. Figure 4.6 shows the aggregate results of the participant responses to inquiry about corporate strategy level UDEs. It shows the findings that small, medium and large business department underperformance and failure to achieve shareholder targets (3.1), together with extreme disruption of financial payment processes (3.2), contribute to wholesale business decline that fails to maximise portfolio outcomes (3.3). These issues are also due to enterprise service technology failure because technology services are under-developed and technology risk is not well managed and disconnected from the enterprise (3.5). Also contributing to these is a failure of organisational culture and reputation, as business units function with an inward-looking silo mentality that takes insufficient account of shared co-dependencies in the business. According to the participants, all of this corporate strategy failure causes a decline in consumer business performance that affects business and consumer confidence in banking (3.0).

Figure 4.6 also illustrates the dynamic and complex nature of mutual and interacting causality in financial institution risk and the UDEs so created. While financial institution risk is mainly inherited from business operations level risk, it can also be negatively compounded by further deterioration of operations due to effects emanating from both business and corporate levels. This means that direction of risk movement can be seen to be bidirectional when viewed from an entire organisation perspective, even though it might appear unidirectional when viewed at a more micro or specific area instance. Elicited through inquiry using the cause–effect–cause TP method with participants, Figure 4.6 shows how risk moves from the bottom up, from operational risk to business risk to corporate risk, where corporate strategy level and business
strategy level UDEs reflect operational shortcomings. In response to inquiry about causes and effects, a silo mentality, where parts of the organisation fail to work together (3.4), was mentioned as a business culture failure. For example, Participant 5 commented on the contrast between the existing silo view of the business and the dynamic nature of risk determinism:

*What we had previously defined as independent risks and effects, they now appear interconnected and they influence each other. This is a highly complex environment that we are operating in at the moment and we have interdependencies that, when you start to think about them, you realise how interconnected everything you're doing is.*

For example, because the multiple risks inherited from the operations level can negatively affect business demand, together with retail operations and compliance issues and a lack of understanding of these (2.0), this can also lead to negative consumer credit and co-branded credit card performance (2.3). Because this is not in alignment with the Australian Retail Credit Association, it results in retail and small business disruptions among emerging and innovative businesses (2.4). These corporate strategy level UDEs inherit risk from these and other business strategy level UDEs.

Also affecting the corporate strategy level, this risk changes the business landscape for both corporate shareholders and executives in terms of leadership and competitiveness. Risk inherited from the operations level significantly affects a business when cards are not properly used or when credit operations are not managed effectively (2.1), which causes underperformance in digital divisions and increased digital disruption among financial institutions (2.6).
The risks caused by operations level product management failures, such as inaccurate balance sheets and liquidity, balance sheet fluctuations and banks having to manage asset/liability mismatch (2.10), can cause financial market declines (2.9) that can result in economic crises or the collapse of long-term speculative bubbles. Such disruptions lead to a decline in corporate performance and productivity (3.1).

Technology operations are directly linked to risk, particularly within the enterprise services division (3.5, 2.12). Risk movement from the operations level through the business strategy level (2.12) into the corporate strategy level (3.5) affects financial technology and legacy systems because integrating these systems into a backend system is difficult. Thus, enterprise services fail on screening and assessment platforms (2.13), and customer service quality declines because staff are not fully prepared to meet customer needs (2.14), resulting in negative business performance (3.4, 3.5). In summary, business risk is caused by disruptions in the frontline of financial institutions’ operations. Such risk is strongly connected to and has a direct impact on overall financial service delivery and institutional reputation, compounding business strategy and corporate strategy level risk.

As corporate strategy level risks are affected by the operations level of financial institutions, this has a negative impact on overall business performance and reputation. For example, retail and small business disruptions among the emerging generation of consumers and innovative businesses (2.4), combined with underperformance in digital and direct growth in the retail division (2.6), negatively affects business and consumer confidence (3.0). Additionally, high business credit risk is caused by borrowers failing to make required payments, lost principal and interest, disruption to cash flows and increased collection costs (2.7), leading to declining performance among corporations and medium and large businesses (3.1). Financial market
decline and complex services (2.9) directly affect wholesale banking (3.3), and poor customer service (2.11) and underperforming digital and direct business (2.14) significantly affect enterprise service performance (3.5).

All the CRTs show the interactions among various risk effect movements between the operations, business strategy and corporate strategy levels of an organisation. Additionally, they show the movement of core risk effects from the customer-facing frontline to the corporate level through the business. The cumulative negative impact of risks throughout the business described by the participants culminated with corporate underperformance and management failure to meet performance targets.

Table 4.5 summarises the main core risk effect types that the CRTs (Figures 4.2–4.6) identified as contributing to the main UDEs. These effect types were interpreted as the most influential, as they were the most commonly mentioned by participants, and their pathways shown in the CRTs (Figures 4.2–4.6) tended to cross into all three functional levels of the institutions and across all business types. These effect types also tended to be located at the junction points of multiple pathways in the combined CRT (Figure 4.6), which provides a view of the organisation in its entirety. This shows that these effect types are likely to be influencing multiple UDEs across the organisation; because of this causal-related connectivity, they are interpreted as the underlying causes of UDEs.

The most influential core effects contributing risk across the business problem domains cluster together under four main core risk effect types: people-centred failures, external service provider disruptions, policy and regulatory compliance limitations, and technology hub failures. Similarly, the participants identified that many risks in product development and IT
arise from poorly controlled risk, as functions outsourced to contracted external service
providers go on to contribute to risk in both retail and business-to-business banking.

Table 4.5 Main underlying core risk effect types

<table>
<thead>
<tr>
<th>Core risk effect types</th>
</tr>
</thead>
<tbody>
<tr>
<td>People-centred failures</td>
</tr>
<tr>
<td>External service provider disruptions</td>
</tr>
<tr>
<td>Policies and regulatory compliance limitations</td>
</tr>
<tr>
<td>Technology hub failures</td>
</tr>
</tbody>
</table>

These underlying risks, although described as types, are not intended to be portrayed as
exclusive of each other. Instead, all these underlying risk effect types were found to constrain
achievement in all four business areas, and contribute to retail banking failing to meet customer
needs, business banking failing to meet targets, product management failures and IT
disruptions. Further, the causal pathways associated with the core or underlying UDEs also
cross over the functional levels of financial institutions (operational level functions, business
strategy level functions and corporate strategy level functions). For example, Participant 4
commented in response to validation questions (see Appendix A) about external provider
disruptions that ‘the push to outsource has produced efficiency benefits but perhaps at a cost
of increased risk that was not foreseen through reduced internal capability to control the risk’.

As described in Section 4.1, the process of participant interview inquiries about UDE causes
and effects was first to iteratively come to a shared view of organisational structural and
functional characteristics (shown in Figures 4.1 and 4.2 respectively). The CRT analyses then
summarised the results of these inquiries, which had elicited UDE causes and effects aligned
with organisational characteristics. Figure 4.7 summarises the risks caused by the main
underlying core risk effect types shown in Table 4.5 mapped onto the functional organisational
structure. It shows the movement of risk through the functional levels of the financial institutions from operational level risk, through to business strategy risks and corporate strategy level risks.

The operations level of the banking organisation represents the area where risk effects are prone to occur. The participants described the operations level as the location of main underlying core risk effect type. From the participant inquiries summarised in the CRT analyses, these were classified as limited human resource (HR) capabilities or people-centred failures, disruptions caused by substandard external services providers, ineffective design policies and regulatory and technology operational failures.

Also shown in Figure 4.7 are operations level risks, such as operating risk, credit risk, customer fairness risk, regulatory risk and compliance risk. The participants agreed that these areas are how financial institutions generally understand types of risk. For example, at the operating level of the organisation, operating risk is the risk of loss resulting from inadequate or failed internal processes and controls, people and systems or external effects. Operating risk, as well as credit, customer fairness, regulatory and compliance risk, arise from the underlying core risk effect types.

The business strategy level risks (see Figure 4.7) are located with the business units located in each division (see also Figure 4.1). In the retail division business strategy level, where demand operations core effect risks occur, the retail and small business units, digital and direct growth units, and asset management and finance units are associated with retail and small business disruption, underperforming digital and direct growth, and asset management and finance complications risk themes respectively.
In the business banking division, where operational supply core risk effects occur, the business strategy level market units, balance sheet and liquidity units and product change units are associated with the risk themes of improper business advice, credit card failures, declines in superannuation, and insurance issues respectively. Risk themes associated with business units in the wholesale banking area where product management risk effects occur are market declines, inaccurate balance sheets and liquidity, and product change issues. The risk themes associated with technology business units are technology failures in customer payments and declines in shared services and business management effectiveness.

The corporate strategy level risks are also shown in Figure 4.7, which shows that financial institution strategic objectives and mission, intended to provide medium-to-longer-term guidance on the direction of the business as a whole, fails to meet expectations. The risks include declines in consumer confidence in retail banking, underperforming small-to-medium business banking, declines in wholesale banking and enterprise technology service failures. As illustrated in the CRTs, the participants portrayed the movement of risk between the levels and across risks within the levels, where different risk features at different parts of the financial institution can reciprocally affect other risks and areas at different levels.
Figure 4.7 Summary of the identified risks mapped to financial institution functional structure
4.3 Summary

This chapter first provided a participant consensus view of the typical or generalised financial institution functions and organisational structure as a template to organise and make sense of the risk faced. This generalised financial institution model was described in Section 4.2 and provided the conceptual organisation for how the results about risk were depicted and institutionally contextualised.

Section 4.3 presented the finding of inquiries with participants regarding the causes and effects of undesired risk effects, progressively through each functional level of the institution and for each major structural or divisional function. These inquiries were validated and triangulated into detailed representations using the TOC CRT method to comprehensive map what was perceived as the current reality of the institutional dynamics of risk. This was undertaken for each of the core effect types to present an integrated and holistic view of the complex determinism of risk, taking account of the functional and structural characteristics of financial institutions identified in Section 4.1 and the nature of risk described in Section 4.3.

In summary, the CRTs (Figures 4.2–4.6) show that customer-facing operational failures (retail, wholesale, products and IT services) have causes related to operational shortcomings, which contribute to various business strategy failures, and these, in turn, compound corporate strategy shortcomings. The CRTs also show the dynamic risk movement through the institutions and illustrate that risk is multidetermined by a complex interacting system of causes. The findings show that risk crosses over onto different functional levels, and is transformed as one type of risk interacts with another and compounded as it moves through organisational structures and functions. In the next chapter, based on the CRT findings, a TOC FRT analysis provides insight
into what the participants thought an effective and desired future might look like, and shows how financial institution risk may be effectively managed.
CHAPTER 5

ANALYSIS AND RESULTS:

FUTURE STATE ANALYSIS

5.1 Introduction

The results of the application of the TP FRT analysis method are described in this chapter. This presents an aggregate view of what the participants considered an effective and desired future, where Australian financial institution risks previously identified in Chapter 4 are effectively managed and controlled. The TP FRT method was described in Section 3.3.3. First, Section 5.2 describes participant consensus on the nature of the risk treatments or injections that they thought would be needed to transform the current risk state and turn it into the desirable future state. Second, Section 5.3 describes the findings of the FRT analysis, which proposes solutions for Australian financial institutions that seek to transform UDEs into DEs; the FRT illustrates the result of the exchanges of the UDEs, previously identified by the TP CRT methods described in Chapter 4, with DEs produced by the hypothetical application of solutions.

Chapter 4 described an aggregate view of what the nine participants from three Australian financial institutions thought was the nature of the risks in Australian financial institutions. This was aligned and informed by the conceptual model of risk core effect types derived from the literature. A detailed analysis using the TP CRT method provided what was perceived as the current reality of the institutional dynamics of risk for each core effect type, to present an integrated view of the entire organisation showing the complex determinism among UDEs, portrayed in the context of the functional and structural characteristics of Australian financial
institutions. These Chapter 4 results form the basis of the analyses and results in this chapter. Utilising the same institutional functional structures (see Figure 4.1) as the CRT findings described in Chapter 4, the FRT analysis in this chapter creates a representation of a desired, improved future state of Australian financial institutions, where risk is portrayed as more effectively managed and controlled by transforming UDEs into DEs.

In summary, the FRT method answers the TP questions ‘What to change?’ and ‘Change to what?’ As described in Section 3.3.3, UDEs previously identified by the CRTs described in Chapter 4 are transformed into DEs by treating the causes of UDEs. Next, the solution treatments (which do not yet exist but are identified as needed to transform the current state into the desirable future state) are described.

5.2 Risk treatments: injections

As described in Sections 3.3.3.3 and 3.3.3.4, the FRT method is intended to assist in overcoming the challenges facing participants regarding how to identify barriers that preclude addressing the cause of a problem. The FRT method seeks to create awareness of solutions to a problem by utilising the logic previously developed in the CRT. The FRT is similar to the CRT, but the hypothetical solutions or actions with potential to transform an UDE into a DE are identified and placed within the tree diagram to illustrate possible future solutions for the issue and to describe a desired future state (Balderstone 1999; Dettmer 1997; Hohmann 2015; Kim, Mabin & Davies 2008). For example, if excessive operational costs are identified by the TP, management may take various steps to reduce costs, which will affect the current reality structure and also have future effects. The FRT identifies possible steps to take to eliminate the effects caused by the introduction of new processes in the future (Hohmann 2015). Through inquiries (Appendix A) undertaken with participants, this FRT method was intended to assist
participants to identify barriers that prevent addressing the cause of a problem, and how to overcome those barriers. It helps in solving the ‘What if?’ questions that arise when a new operation with a remedial purpose is introduced into a system. The FRT portrays the use of these new operations, called injections. Injections are actions or something new or done differently that have the effect of neutralising the effects of the UDEs and converting them into DEs (Balderstone 1999; Dettmer 1997; Hohmann 2015; Kim, Mabin & Davies 2008). In summary, the FRT method is intended to show the effect of exchange of the UDEs with DEs through the application of injections.

Before an FRT analysis is undertaken, a list of potential injections to be tested and then illustrated in the FRT analysis is first elicited from the participants. As part of the future state phase of the research and interview process described in Section 3.5 and inquiry semi-structured questions shown in Appendix A, the participants were prompted about a desired future regarding the treatment of organisational risk related problems. These injections were collated into a list by the researcher, with adjustments to terminology to reflect an aggregated consensus view, and then reflected back to the participants for validation as part of the research steps described in Section 3.5. These were then used as the injections to be mapped as part of the FRT methods of inquiry.

The injections are described over the three levels of major institutional functions (see Figure 4.1), comprising the operations level (Section 5.2.1), business strategy level (Section 5.2.2) and corporate strategy level (Section 5.2.3). Although not mutually exclusive nor independent, the purpose of organising the injections according to these functional levels of the financial institution was to facilitate the systematic inquiry of the FRT method to ensure an entire organisational view. Like the CRT method and approach described in Chapter 4, the
information from all three financial institution cases and the nine participants was aggregated into a single generic view judged by the participants to be representative of typical or generic Australian financial institutions, which comprise banking services as a major part of the financial products and services mix offered. The injections were described by the participants to reflect a consensus view of the contemporary risk-related practice terminology in use in Australian financial institutions among staff who have a predominantly risk-related role.

5.2.1 Operations level related injections

5.2.1.1 Operations injection 1: Operations actions

This injection refers to the implementation of an action plan comprising several potential tactical actions intended to transform UDEs and their precursors into DEs and whatever prerequisites might be required for the transformation. For example, Participant 3 mentioned people-centred capacity and capability related actions to remediate people-related failure effects:

that would include error, lack of training, lack of capability. You know, pandemic–
all of those sort of things– we need enough people, and to build their capacity and
capability– all those sorts of things related to people skills that causes issues across
the board.

Actions in this example could include improvements to recruitment processes, improved training and professional development, improved people-related policies and procedures, job redesign and work value reviews. The particular UDE and its underlying causes would be examined to determine what action would best transform it into a DE. The design of the action plan uses multiple sources of input, such as CRT findings and the outputs of the other injections. For example, the action plan would be designed by the control centre (Section
5.2.1.3) using intelligence gained from operations assessment (Section 5.2.1.2), the risk library (Section 5.2.1.6) and the risk register (Section 5.2.1.4), together with information collated, synthesised and shared through the operations monitoring and reporting centre (Section 5.2.1.5).

5.2.1.2 Operations injection 2: Operations assessment

This injection includes diagnostic recommendations about operational strategies and responses to the current risk. This arises from where risks have been identified, categorised and assessed by likelihood of occurrence and possible severity of the impact of the consequence of an occurrence. Together, these indicate whether the investment into the response to the risk should be mandatory or allowed to be discretionary. For example, a number of participants suggested that where an impact involved likely failure to adhere to a regulatory requirement, responses should more likely be required to be mandatory. Operations injection 2: operations assessment is the injection function where this kind of assessment is undertaken.

5.2.1.3 Operations injection 3: Operations control centre

This injection delivers a comprehensive view of the status of risk control across the operations of the financial institution and designs the action responses to reduce risk. Using combined intelligence from multiple sources including the information outputs of the other information collection, classification and repository related injections, it facilitates a full understanding of risk, including the design and implementation planning for operations injection 1: operations actions. It enables adaptive prioritisation of risk control tactical actions. For example, if an injection element does not work as intended, the control centre provides a clear indication of whether the process or control is effective or not, and what further remedial action is required.
5.2.1.4 Operations injection 4: Operations risk register

The *operations risk register* injection is a sortable list that identifies risks, which are then classified and catalogued according to a fit-for-organisational purpose taxonomy of common risk types and domains. It also contains resources to help institution risk practitioners conduct a qualitative risk assessment of the items listed in the register. It is intended to support a strategic and holistic appreciation of risk and to inform risk assessment and tactical remedial action design and implementation planning.

5.2.1.5 Operations injection 5: Operations monitoring and reporting centre

The *operations monitoring and reporting centre* helps to assess and monitor risk in frontline customer-facing operations. It identifies new risks and the planning for them, keeps track of existing known risks to check if a reassessment is necessary, notes if any risk conditions have been triggered, and monitors risks that could become more critical over time. It also tracks remaining risks that may require a longer-term, planned, and managed approach with risk action plans, and reclassifies risk based on new or updated information. For example, this includes risks that are ongoing and cannot be closed, where ongoing criticality needs to be monitored. The *operations monitoring and reporting centre* monitors the effects of the implementation of an action plan over time. This enables the action plan or other injection effectiveness to be assessed and determines whether it should be re-examined.

5.2.1.6 Operations injection 6: Operations risk library

The *operations risk library* is used to save and record information on operations level risks. It summarises and defines, in a common repository, risks to which the financial institution is exposed. The library helps to facilitate discussions of risks and their definitions, and promotes both consistency and a culture of risk awareness. It is a resource that stores information about various processes, sub-processes, operational risk effects and control types across the
institution’s businesses. For example, it is the repository for the processes of risk assessment and measurement, risk effect definition and information about the links of business unit results to institutional performance. The library repository enables more effective risk management and improvement by keeping records and information about defining and identifying the types of risks and various risk effects, defining and identifying specific controls, assessing and rating the controls, and supporting other monitoring and risk reporting and documentation needs. It is the institution’s durable ‘organisational memory’, which facilitates retention and development of risk management capability. Next, five injections operating at the business strategy functional level of Australian financial institutions are described.

5.2.2 Business strategy level injections

5.2.2.1 Business strategy injection 1: Business risk library

The business risk library records all business strategy level risk related information. It has the same functions as operations injection 6: operations risk library described in Section 5.2.1.6 but the repository content includes risk information concerning the business strategy level of the organisation.

5.2.2.2 Business strategy injection 2: Business actions

Similar to operations injection 1: operations actions regarding control actions described in Section 5.2.1.1, this injection refers to the design and implementation of an action plan comprising potential tactical actions needed to transform UDEs located at the business strategy level and their precursors into DEs.

5.2.2.3 Business strategy injection 3: Business assessment

Similar to operations injection 2: operations assessment described in Section 5.2.1.2, but with a focus on business strategy level functions, this injection includes recommendations about
business strategies and responses to the current risk, based on risks having been identified, categorised and assessed by likelihood of occurrence and possible consequence of an occurrence. Together, these indicate whether the response to the risk should be mandatory.

5.2.2.4 Business strategy injection 4: Business control centre
Similar in nature to operations injection 3: operations control centre (Section 5.2.1.3), and operating in conjunction with it, this injection delivers a comprehensive view of the status of risk control across the business strategy level functions of the financial institution.

5.2.2.5 Business strategy injection 5: Business monitoring and reporting centre
Working in conjunction with operations injection 5: operations monitoring and reporting centre described in Section 5.2.1.5, the business monitoring and reporting centre helps assess and monitor risk behaviour in the decision-making levels of the divisions of the business. It helps to assess and monitor risk behaviour regarding business strategy. It identifies new risks and the planning for them, keeps track of existing risks to check if reassessment is necessary, monitors risk conditions that may have been triggered, and monitors risks that could become more critical over time. It also tracks remaining risks that may require a longer-term, planned, and managed approach via risk action plans, and reclassifies risk based on new or updated information.

Finally, three proposed injections at the corporate strategy functional level of each of the four core risk effects areas in financial institutions are described.

5.2.3 Corporate strategy level injections
5.2.3.1 Corporate strategy injection 1: Risk appetite
This injection comprises modification of the amount and type of risk for which the financial institution is prepared to pursue reduction or to retain. Risk appetite influences the core risk
effects and the organisational system of interacting causal dynamics illustrated in the CRTs. This injection indicates the risk policy settings at the corporate level at which the business can accept or reject a course of action, and whether the related decisions facilitate or inhibit the attainment of organisational objectives and mission. To illustrate, Participant 8 observed that:

The way I see it, the common denominator across credit risk, operational risk, all these types of risk, is the risk management framework that sits in its own bubble and that drives issue management, change management, obligation adherence, compliance adherence, operational risk business environment, definition, and how I said what the most important thing is would be risk appetite settings at the very top. That appetite framework drives all this interaction and provides input into process improvement after the fact.

5.2.3.2 Corporate strategy injection 2: Cultural adaptation

This injection concerns corporate-led implementation strategies to improve relationships with supply chain business partners and both business and consumers through enhanced intercultural awareness and adapting to both global and multicultural contexts. It also refers to complementary internal-facing strategies that improve cooperative and supportive relationships among business units and functional levels of the financial institution to both improve organisational climate and promote proactive management and prevention of risk. The importance of creating a cultural context was emphasised by Participant 7 who observed that:

If you're getting the full value chain, working together, owning responsibility. That comes down to your cultural adaption, so you've got to make sure that culturally that is seen as the preferred direction.
5.2.3.3 Corporate strategy injection 3: Collaboration centre

This injection concerns the creation of the mechanisms that facilitate cross-area cooperation, information exchange, organisational values and the establishment of a corporate culture of shared responsibility for the mitigation of risk. It comprises approaches that enable cross-functional engagement and creates the conditions that reduce the UDEs of business unit structures that operate independently and in an isolated way, where the failure to effectively collaborate leads to decisions and conditions that promote risk. Participant 4 noted the need for organised effort for risk reduction collaboration in large financial institutions:

*And then cross divisional collaboration. It's very difficult. I don't think any company has got that down pat. It's too difficult ... To get uniformity, whether it's in processes, whether it's in procedures, whether it's in reporting, is very difficult and takes a deliberate and planned effort.*

The next section illustrates how the injections described above are intended to transform UDEs to DEs. The FRTs illustrate the future state that an organisation desires to achieve arising from the proposed implementation of the injections in each core risk domain areas and for each of the three functional levels of financial institutions (operations, business strategy and corporate strategy).
5.3 Future reality tree analysis

Whereas the CRT method identified the root cause of the problem from the UDEs, the FRT method portrays the effect of using injections. Described in Section 5.2, injections are actions or something new or done differently that have the effect of neutralising the effects of the UDEs and converting them into DEs. The FRT illustrates the exchange of UDEs with DEs through the application and effects of injections. FRTs are constructed in this section to test the effects of the proposed injections located in each of the three functional levels of financial institutions (operations, business strategy and corporate strategy). The FRT is constructed from the CRT for each core risk domain area described in Chapter 4.

Whereas the CRTs in the previous chapter explained and mapped the causes of risks or obstacles in financial institutions, each FRT ‘injects’ various remediation elements to illustrate the logic of how they mitigate the problematic impact of the different risks. Participant observations in response to inquiry questions (see Appendix A) about the application of injections to transform undesired risk effects occurring at each functional level of the organisation into DEs were determined and validated with the participants.

In summary, the FRT illustrates the logic of how injections are used to neutralise the effects of UDEs and convert them into DEs. For example, poor service provided by people-centred services or the HR department can be changed via better remuneration, job training and good supervision to create the desired effect of high-quality service provision. Four FRTs are presented, one for each of the four core risk domain areas also used for the CRTs in Chapter 4 where the core UDE is transformed into a desirable effect. The domain areas are demand in retail banking (Figure 5.1), supply in business banking (Figure 5.2), product management (Figure 5.3) and IT (Figure 5.4).
5.3.1 Future reality tree for demand in retail banking

This section describes the findings from inquiries with participants about how the UDE of retail banking failing to meet customer needs, described in Section 4.3.1 and illustrated in Figure 4.2, is transformed into a desired future state where customer needs are met. Participant observations in response to inquiry questions (see Appendix A) on the application of injections to transform undesired risk effects occurring at the operational functional level of the organisation into DEs were aggregated into the FRT and validated with the participants. These aggregated findings of the inquiry process are illustrated in Figure 5.1, which shows the expected effects on Australian financial institution retail banking when the injections described in Section 5.2 are implemented to eliminate or mitigate the undesired risk effect of retail banking failing to meet customer needs (Section 4.3.1).

*Operations injection 1: operations actions* (see Section 5.2.1.1) comprises a range of operational level tactical actions in the retail banking area strategically applied to a variety of operational elements to maximise impact and reduce risk vulnerability. These are applied to increase the effectiveness of staff induction and training (1.3), which, in turn, improves retail capacity to meet needs (1.5), continued professional development (1.14) and improved recruitment (1.11). Improved recruitment (1.11) also increases the capacity and capability of HR functions (1.8). As a consequence of improved retail capacity to meet needs (1.5), policy and procedures (1.15) to guide people-centred operations is improved. Resulting also from the effect of *injection 1: operations actions*, less pressure on retail staff (1.4) contributes to more effective HR policy and procedures (1.15). The indirect effects of *injection 1: operations actions*, which resulted in improvements in retail capacity and support (1.5), went on to also increase the capacity and capability of HR or people-centred functions (1.8), and to
contribute to more effective business monitoring and evaluation (1.12). Participant 2 highlighted people-centred improvement:

"Capacity and capability are what comes to mind. Where you've got here—branch staff capability—it's part of that and I do see it coming from supply issues. We're also talking about capacity? Across our point of view, I see those are the main drivers for HR issues. From a capability and a capacity. You need to manage those two things in HR."

Injection 1: operations actions also improve phone banking services provision (1.7) and hardware and software practices (1.1), which, in turn, improves electronic services including further improvement in phone banking (1.7), online banking uptake (1.2), EFT functions (1.10), as well as improved compliance (1.13) and better business monitoring and evaluation (1.12). Electronic services improvements result in more customers using online services (1.2) and branch customers are more satisfied (1.9).

All of these improvements either directly or indirectly resulting from injection 1: operations actions were designed, supported and made more effective through the combined effects of the complementary injections comprising injection 2: operations assessment (Section 5.2.1.2), injection 4: operations risk register (Section 5.2.1.4) and injection 6: operations risk library (Section 5.2.1.6), where an effective injection 3: operations control centre (Section 5.2.1.3) provided implementation guidance and coordination of the changes.
Figure 5.1 Future reality tree for demand in retail banking
Overall, injection 5: operations monitoring and reporting centre (Section 5.2.1.5) provided overall monitoring of risk behaviour in frontline operations to feedback intelligence to the other injection functions to adapt to changes where needed to continue to mitigate risks and obtain the DEs. For example, Participant 5 suggested that ‘to avert risk effects in retail you need to have the control capacity in place to identify and respond before it occurs to prevent it’.

Figure 5.1 also shows business strategy injection 2: business actions applied to the business strategy level of demand in retail banking. Together with improvements arising from the operations level injections, including changes in various people-centred or HR functions (1.14, 1.15) and other operations level improvements (1.1, 1.11, 1.12, 1.13), as well as information from the other operations injections including operations injection 6: operations risk library and operations injection 5: operations monitoring and reporting centre, business strategy injection 2: business actions included tactical actions that together improved responses to innovation (2.5), performance of digital and direct growth of retail (2.6), better managed credit risks (2.7) and contributed to financial market performance (2.8), and contributed to increases in customer service levels and quality (2.12). Business strategy injection 4: business control centre also contributed to better managed credit risks (2.7) through tighter risk controls.

The improved operational level influences (1.12, 1.13, 1.14, 1.15), together with the influence of business strategy injection 3: business assessment, contribute to the improved quality of staff advice (2.2), which, in turn, improves consumer business confidence (2.11), increases investment and corporate performance for debt and equity (2.3), and improves management of high credit risk (2.7). The effect of the business handling credit operations well (2.1), which was improved by operational level improvements such as regulatory compliance adherence
(1.13), contributes to growth in the retail division (2.6) and improved credit performance (2.4), which, in turn, together with *business strategy injection 2: business actions*, stimulates innovation in retail and small business (2.5) and contributes to improved retail growth (2.6). Risk arising from the complexity of legacy systems, which was controlled through operational level policy and procedures (1.15) and improvements in the effectiveness of business monitoring (1.12), leads to increased confidence in consumer business performance (2.11) and contributes to a well-performing financial market (2.8). Improved consumer business performance (2.11), together with increased customer service satisfaction (2.9), combined with the effect of *business strategy injection 2: business actions*, lead to increases in customer service level quality (2.12).

At the business strategy level overall, *business strategy injection 5: business monitoring and reporting centre*, supported by intelligence stored and accessed from *business strategy injection 1: business risk library*, provided overall monitoring of risk behaviour in business units strategies and their effectiveness. This is intended to feedback intelligence to inform the other injection functions and to adapt to changes where needed to continue to mitigate risks and obtain the DEs. Participant 5 noted:

*The need for a consolidated view where for each performance unit, it does have an effective control environment in place to mitigate the risks. You need to have a reporting and collaboration centre between the business and the corporate level of the organisation.*

The corporate strategy level injections of risk appetite modification (*corporate strategy injection 1: risk appetite*) and cultural adaption improvement (*corporate strategy injection 2: cultural adaptation*) both led to higher consumer business performance (3.0), contributed to
meeting shareholder performance targets (3.1) and better wholesale portfolio outcomes (3.2),
and improved enterprise technology (3.3). Improvement in these were also helped by business
strategy level effects through retail and small business improvements (2.5), retail growth (2.6),
and better management of credit risks (2.7), as well as improved financial market performance
(2.8) and better customer service levels and quality (2.12). Improvement in cross-area cooperation, information exchange, organisational values and the establishment of a corporate
culture of shared responsibility for the mitigation of risk through the efforts of the collaboration
centre (*corporate strategy injection 3: collaboration centre*) also contributed to the creation of
the DEs. Together, better understanding of shareholder expectations and consumer needs when
engaging both business strategy and operations provides clear direction and quick response to
risks provided through the combined effects of the injections.

In summary, this section showed the effect of injections applied at three functional levels of
the financial institutions in the retail banking domain, which had UDEs contributing to the
UDE of failing to meet customer needs. In Chapter 4, the most influential types of core risk
types found to contribute to this failure were people-centred failures in the retail platform,
external service provider disruptions, retail policies and regulatory limitations, and retail
technology hub failures. The demand in retail banking FRT (see Figure 5.1) showed how a
range of injections (Section 5.2) transformed these contributing UDEs into DEs, with the
combined effect of retail banking meeting customer needs. The FRT findings showed that the
effects of the injections were a result of their combined effects at multiple leverage points
across the institution corresponding to each of the main core risk areas and at each functional
level. Further, in addition to the direct effects of the injections, the DEs created a flow-on
improvement influence on other effects, and when combined with injection effects, also co-
contributed to other UDEs’ transformation into DEs.
5.3.2 Future reality tree for supply in business banking

This section describes the findings from inquiries with participants about how the UDE of business banking (business-to-business banking including wholesale banking services) failing to meet business-to-business targets, which was described in Section 4.3.2 and illustrated in Figure 4.3, is transformed into a desired future state where the targets are met. Participant observations in response to inquiry questions (see Appendix A) about the expected effects of the application of injections to transform undesired risk effects occurring at the business strategy functional level of the financial institutions into DEs were aggregated and validated with the participants. The findings of this inquiry process are illustrated in Figure 5.2, which shows the expected effects on Australian financial institution business banking when the injections described in Section 5.2 are implemented to eliminate or mitigate the UDE of business banking failing to meet business targets (Section 4.3.2).

The expected effects on the financial institution operations level are shown in Figure 5.2, where the six operations level injections described in Section 5.1 are implemented to eliminate or mitigate expected risks arising from the failure of business banking to meet business targets (1.0). *Operations injection 1: operations actions* comprises a range of tactical actions strategically applied to a variety of operational elements to reduce risk vulnerability by transforming UDEs into DEs. The effects of *operations injection 1: operations actions* included more effective policy and governance (1.10), resources provided to meet business-to-business needs (1.5), staff meeting business-to-business needs (1.7) and improved recruitment processes (1.13).

These desired effects, in turn, led to improved HR capability to support the business (1.9) and to more effective professional development and training (1.17) and improved people-centred...
policies and procedures (1.18). Also, through improved recruitment (1.13) and improved technology operations (hardware and software) capability (1.2), there was improved internet and phone services (1.1, 1.3), with flow on to business monitoring and evaluation (1.15) improvements. These improvements were designed, supported and made more effective through the combined effects of the complementary injections comprising operations injection 2: operations assessment, operations injection 4: operations risk register and operations injection 6: operations risk library, where operations injection 3: operations control centre provided guidance and coordination for the changes.

Overall, operations injection 5: operations monitoring and reporting centre provided oversight monitoring of risk of business-to-business operations to feedback intelligence to the other injection functions to adapt to changes where needed to continue to mitigate risks and to obtain the DEs.

Figure 5.2 also shows the effects of business strategy level injections applied to business banking. Together with improvement arising from operations level people-centred improvements (1.13, 1.17, 1.18) and other operational level improvements (1.15, 1.16), these led to improved credit performance (2.2), which then led to improved innovations in small business (2.3) and better handling of credits operations (2.0) and better business advice from staff (2.1).
Figure 5.2 Future reality tree for supply in business banking
As well as information gained from the other operations level injections (recorded in *business strategy injection 1: business risk library*, *business strategy injection 3: business assessment* informed the tactical actions (*business strategy injection 2: business actions*) that together improved innovation (2.3), performance of digital and direct growth of retail (2.4), and better managed credit risks (2.6) and contributed to financial market performance (2.7). Also improved by better business advice (2.1), improved management of asset–liability risks (2.8) contributed to improved financial market performance (2.7). The improved operational influences (1.12, 1.15, 1.18), combined with the effects of the business injections and the improved quality of staff advice (2.1), improved the ability to control the complexity of interfaces with legacy systems (2.10), leading to other technology improvements (2.11) with increases in customer service levels and quality (2.12) and satisfaction (2.9). Overall, *business strategy injection 5: business monitoring and reporting centre* provided overall monitoring of risk behaviour in business units strategies to feedback intelligence to the other injection functions. This allowed responsive adaption to changes where needed to continue to mitigate risks and obtain the DEs. For example, Participant 3 reported:

> Effective collaboration and monitoring are critical elements in the central role of the interface between the corporate side of the business and can have real impacts on operational risks. Risk mitigation action that is well coordinated, mutually informing and communicated can have a positive effect on things like training, recruitment, customer service levels and innovation. You really need a strongly connected and aligned supporting context that is cross-functional ...

The corporate injections of risk appetite modification (*corporate strategy injection 1: risk appetite*) and cultural adaption improvement (*corporate strategy injection 2: cultural
adaptation) both led to higher consumer business performance (3.0), and contributed to meeting shareholder performance targets (3.1), better wholesale portfolio outcomes (3.2) and improved enterprise technology (3.3). Improvement in these were also helped by, and, in turn, influenced, business and operations effects.

Improvement in organisational culture through the establishment of a corporate culture of shared responsibility for the mitigation of risk through the efforts of the collaboration centre (corporate strategy injection 3: collaboration centre) also contributed to the creation of the DEs. Together, better understanding of shareholder expectations and large business consumer needs can have a significant impact on a financial institution’s productivity; however, adaptive rebalancing of business financial risk appetite also contributes to productivity and improved collaboration helps avoid both expected and unexpected risks.

In summary, this section showed the effect of injections applied at three functional levels of the financial institutions in the supply in business banking domain, which had UDEs contributing to the UDE of failing to meet business-to-business targets. In Chapter 4, the most common types of core risks found to contribute to this failure of supply in business banking were people-centred failures in business operations, external service provider disruptions, policies and regulatory limitations, and technology hub failures. The demand in business banking FRT (Figure 5.2) showed how a range of injections (Section 5.1) transformed these contributing UDEs into DEs, with the combined effect of business banking meeting business-to-business targets. The FRT findings showed that the effects of the injections were a result of their combined effects at multiple leverage points across the institution, corresponding to each of the main core risk areas and each functional level. Further, in addition to the direct effects
of the injections, the DEs created flow-on improvement influences on other effects, and when combined with injections effects, co-contributed to other UDEs’ transformation into DEs.

5.3.3 Future reality tree for product management

This section describes the findings from inquiries with participants about how the UDE of product management failures, described in Section 4.3.3 and illustrated in Figure 4.4, could be transformed into a desired future state where product management is successful. Participant observations in response to inquiry questions (see Appendix A) about the expected effects of the application of injections to transform undesired risk effects occurring at each functional level of the financial institutions into DEs were aggregated and validated with the participants. The findings of this inquiry process are illustrated in Figure 5.3, which shows the expected effects on Australian financial institution product management when the injections described in Section 5.2 are implemented to eliminate or mitigate the UDE of product management failure (Section 4.3.3).

The operations injection 1: operations actions to transform UDEs contributing to product management failures into DEs is guided through the establishment of an operations injection 3: operations control centre that provides coordination to reduce risk vulnerability. That led to improved people-centred capacity and capability to support the business (1.15), leading to more effective policy and governance (1.14), professional development (1.13), and contributed to more effective business monitoring (1.11). These injections also led to more controlled product resources (1.10), which better fulfilled audit and regulatory requirements (1.12) and contributed to professional development improvement (1.13).
Figure 5.3 Future reality tree for product management
Also, through improved recruitment (1.17) and improved technology services and operations capability and functions (1.1, 1.2, 1.6, 1.17, 1.18, 1.19), there was improved internet and phone services (1.4, 1.5), and with technology improvements, better business monitoring and evaluation (1.15). All of these improvements were informed by risk information, supported and made more effective through the complementary injections, comprising operations injection 2: operations assessment, operations injection 4: operations risk register and operations injection 6: operations risk library, which provided intelligence to the operations injection 3: operations control centre, enabling coordination of the transformations by the operations injection 1: operations actions. Also, as product management became more successful, customers coming into branches were more satisfied (1.9). Overall, the operations injection 5: operations monitoring and reporting centre provided overall monitoring of risk behaviour regarding product management related operations to feedback intelligence to the other injection functions to adapt to changes where needed to continue to mitigate risks and obtain the DEs.

Figure 5.3 also shows the business strategy injections (Section 5.2.2) applied to the business strategy level of product management functions to produce key improvements in strategic business unit risk contributing to product management failures. Together with improvements arising from operations level changes in various people-centred functions (1.13, 1.14) and other operational improvements, as well as risk information collated from the operations level through the operations injection 5: operations monitoring and reporting centre and informing business strategy injection 3: business assessment, business strategy injection 2: business actions included tactical actions that together led to improved responses to innovation (2.7) and performance of digital and direct growth of retail (2.8), through better managed credit risks
With positive influence from operational level improvements (1.11, 1.12, 1.13, 1.14), better business advice from staff (2.1) and better handling of credit operations (2.0) also contributed to reduced credit risk (2.9) and led to retail growth (2.8) respectively. Together with other influences (1.11, 1.14, 1.16) and business strategy injection 3: business assessment, better advice (2.1) also led to more accurate balance sheets (2.2) and improved enterprise development (2.5).

In turn, more accurate balance sheets (2.2) and more effective management of legacy systems management contributed to improved financial market performance (2.10). The improved operational influences, together with business strategy injection 3: business assessment, business strategy injection 1: business risk library and business strategy injection 4: business control centre, also improved the quality of staff advice (2.1), and the ability to control the complexity of interfaces with legacy systems (2.4), leading to other technology improvements (2.5) with increases in customer service levels (2.11). Overall, the business strategy injection 5: business monitoring and reporting centre provided overall monitoring of risk behaviour regarding business units’ strategies to feedback intelligence to the other injection functions to adapt to changes where needed to continue to mitigate risks and obtain the DE of success in product management.

Together with business strategy level improvements (2.7, 2.8), the corporate strategy level injections corporate strategy injection 1: risk appetite modification and corporate strategy injection 2: cultural adaptation improvement both led to higher consumer business performance (3.0), and contributed to meeting shareholder performance targets (3.1), better wholesale portfolio outcomes (3.2) and improved enterprise technology (3.3). Improvement in these were also both helped by, and, in turn, influenced, business and operations effects.
Participant 2 noted that ‘it's important that communication and messaging comes from the top. Communications and messages, some of the policies and messages that get rolled out has to come from the top and then that disseminates across the organisation’.

Improvement in organisational culture through the establishment of a corporate culture of shared responsibility for the mitigation of risk through the efforts of the corporate strategy injection 3: collaboration centre also contributed to the creation of the DEs. Together, better understanding of shareholder expectations and business consumer and wholesale needs can have a significant impact on a financial institution’s productivity. However, rebalancing business financial risk appetite also helps, and improved collaboration helps avoid expected risks in product management as well as other core risk effect types. For example, Participant 1 stated:

*The effective implementation of corporate risk appetite driven control over product risk is often blocked or reduced by a silo mentality of individual areas. They go about their business somewhat disconnected from controls whose intention is to monitor and moderate risks, but these intentions often don’t bear fruit because of the disconnects, and can cause issues I’ve seen with swapping exchange rates for example.*

In summary, this section showed the effect of injections applied at three functional levels of the financial institutions in the product management domain, which had UDEs contributing to the UDE of product management failure. In Chapter 4, the most common types of core risks found to contribute were product and market-centred failures, product and external service provider disruptions, product and market policy and regulatory limitations, and product and market technology hub failures. The product management
FRT (Figure 5.3) showed how a range of injections (Section 5.2) transformed these contributing UDEs into DEs, with the combined effect of product management success. The FRT findings showed that the effects of the injections were a result of their combined effects at multiple leverage points across the institution, corresponding to each of the main core risk areas and each functional level. Further, in addition to the direct effects of the injections, the DEs created a flow-on improvement influence on other effects, and when combined with injection effects, co-contributed to other UDEs’ transformation into DEs.

5.3.4 Future reality tree for information technology

This section describes the findings from inquiries with participants about how the UDE of IT issues disrupting the business of the financial institution, described in Section 4.3.4 and illustrated in Figure 4.5, could be transformed into a desired future state where IT effectively supports the business. Participant observations in response to inquiry questions (see Appendix A) about the expected effects of the application of injections to transform undesired risk effects occurring at each functional level of the financial institutions into DEs were aggregated and validated with the participants. The findings of this inquiry process are illustrated in Figure 5.4, which shows the expected effects on Australian financial institutions when the injections described in Section 5.2 are implemented to eliminate or mitigate the undesired effect where IT disrupts the business (Section 4.3.4).

The application of operations injection 1: operations actions to undesired IT failure related effects is guided through the establishment of an operations injection 3: operations control centre and informed by operations injection 2: operations assessment to provide intelligence, guidance and coordination to reduce risk vulnerability by transforming UDEs into DEs. With improved management of hardware and software issues (1.1), ATMs better meet customer
demand (1.8), electronic funds processing is more effective (1.7), and phone (1.4) and online banking (1.2) services are improved, leading to more effective customer transactions (1.19), more satisfied customers (1.6) and improved uptake of online services (1.3). Improved technical systems (1.1) improve business monitoring support (1.16), and people-centred capacity and capability is improved through access to better and more reliable internal systems (1.14). Better systems (1.1) also assist in fulfilling compliance requirements (1.17).

In addition, as a result of operations injection 1: operations actions, the capacity and capability of people-centred functions is further improved, with flow-on benefits to improved professional development (1.18) and, with other DEs (1.1, 1.13), more effective business monitoring (1.16). More effective HR policy and governance (1.18) and professional development (1.17) from improved people-centred capability (1.18) leads to improved recruitment (1.10) and improved technology operations capability and functions (1.1). All of these improvements were designed, supported and made more effective through the complementary injections comprising the operations injection 4: operations risk register and operations injection 6: operations risk library, where an effective operations injection 3: operations control centre provides guidance and coordination for the changes. As technologies become more reliable in meeting needs, and together, improve customer satisfaction (1.9), applications use (1.9) and other technical services improve (1.7), with less error (1.5). Overall, the operations injection 5: operations monitoring and reporting centre provided overall monitoring of risk behaviour regarding frontline operations to feedback intelligence to the other injection functions to adapt to changes where needed to continue to mitigate risks and obtain the DEs.
Figure 5.4 Future reality tree for information technology
Figure 5.4 also shows the injections applied to the business strategy level of the financial institution to produce improvements in strategic business unit risk contributing to minimising IT disruptions. Improvements in business strategy level functions arise from operations level improvement changes (1.16, 1.17) that mean that credit card operations were well handled (2.0), and improvements (1.16, 1.17, 1.18) leading to improved business advice from staff (2.1). When these (2.0, 2.1) are combined with the business strategy level injections, including business strategy injection 2: business actions and business strategy injection 3: business assessment, these together increased investment and corporate performance for debt and equity (2.5), improved insurance and superannuation use of digital technology (2.6), responses to the performance of digital and direct growth of retail (2.7), and better managed credit risks (2.8) and contributed to financial market performance (2.9).

The improved operational level influences (1.8, 1.12, 1.15, 1.16), together with improved quality of staff advice (2.1), improved the ability to control the complexity of interfaces with legacy systems (2.3), leading to other technology improvements (2.4) with increases in customer service levels (2.10). Increases in customer service levels (2.10) were also improved by operations level improvements (1.2, 1.4, 1.7, 1.19). Overall, the business strategy injection 5: business monitoring and reporting centre provided overall monitoring of risk behaviour regarding business units’ strategies to feedback intelligence to the other injection functions to adapt to changes where needed to continue to mitigate risks and obtain the DEs.

The corporate injections of corporate strategy injection 1: risk appetite modification and corporate strategy injection 2: cultural adaptation improvement led to higher consumer business performance (3.0) and contributed to meeting shareholder performance targets (3.1), better wholesale portfolio outcomes (3.2) and improved enterprise technology (3.3).
Improvement in these were also both helped by, and, in turn, influenced by both business strategy level and operations level effects. Improvement in organisational culture through the establishment of a corporate culture of shared responsibility for the mitigation of risk through the efforts of the corporate strategy injection 3: collaboration centre also contributed to the creation of DEs related to technology services supporting the financial institution in the achievement of strategic objectives. Participant 7 provided this perspective on both corporate leadership and external service providers regarding the nature of risk in the delivery of enterprise technology services:

*More leadership around reinforcing a view of IT external service providers, internal business needs and IT system integration should be more driven by delivering information that supports business decision-making rather than an unbalanced focus on isolated technical risks. You know, having a connected risk control soft-infrastructure in place is necessary to mitigate risk in the hard enterprise infrastructure.*

In summary, this section showed the effect of injections applied at three functional levels of the financial institutions in the IT domain, which had UDEs contributing to the UDE of IT business disruptions. In Chapter 4, the most common types of core risks found to contribute were IT systems people-centred failures, external service provider disruptions, policy and regulatory compliance limitations, and technology hub failures. The IT FRT (Figure 5.4) showed how a range of injections (Section 5.2) transformed these contributing UDEs into DEs, with the combined effect of IT effectively supporting the business. The FRT findings showed that the effects of the injections were a result of their combined effects at multiple leverage points across the institution corresponding to each of the main core risk areas and each
functional level. Further, in addition to the direct effects of the injections, the DEs created flow-on improvement influence on other effects, and when combined with injection effects, co-contributed to other UDEs’ transformation into DEs.

5.3.5 Overall institutional perspective of injections

In Section 4.3.5, a whole-of-organisation perspective summarising the findings on the causes and effects of UDEs was provided. Figure 4.7 provided a summary of the Chapter 4 current state CRT findings mapped to a generic financial institution structure. Similarly, Figure 5.5 provided a whole-of-financial-institution view of the findings of the FRT method regarding the application of injections where the current state (shown by the CRTs in Sections 4.3.1–4.3.5) is transformed into a desired future state (the FRTs described in Sections 5.3.1–5.3.4). Figure 5.5 shows the injections (Section 5.2) and how they are located and organised, taking into account both the functional and structural characteristics of the organisation, as described in Chapter 4. To summarise, Figure 5.5 illustrates the results of the FRT findings, mapped to the same organisational structure as the CRT findings illustrated by Figure 4.7, where the latter is transformed into the former through the effects of the injections.

In Figure 4.7, the underlying core risks effect types are shown as being the foundation for operational level risks, moving up to create business strategy level risks, before manifesting as corporate strategy level risks. In Figure 5.5, these core risk effect types (shown in Table 4.5 and described in Section 4.3.5) are also shown, and include people-centred failures, external service provider disruptions, policy and regulatory compliance limitations, and technology hub failures. In Figure 5.5, the injections that control these core UDE risks are shown at each functional level of the financial institution (operations, business strategy and corporate strategy).
Also shown are each major divisional structure associated core effects, comprising demand in retail, supply in business banking, product management and IT. At the business strategy level, the UDEs or risks associated with the divisional business units are shown, together with the major strategic objectives associated with each division at the corporate strategy level. Aligned with each of these institutional functional and structural characteristics, Figure 5.5 shows the organisational location of the injections described in the Section 5.2 and whose effects were illustrated in Figures 5.1–5.4.

At the operations level, the injections operations actions (Section 5.2.1.1), operations assessment (Section 5.2.1.2), operations control centre (Section 5.2.1.3), operations risk register (Section 5.2.1.4), operations monitoring and reporting centre (Section 5.2.1.5), and operations risk library (Section 5.2.1.6) are shown. Aligned with each of the core risk effect types, the operations risk library is the risk intelligence repository for risk controls, operations assessment and operations risk register for each of the core risk effect types, comprising people-centre failures, external service providers disruption, policy and regulatory limitations, and technology hub failures. The operations monitoring and reporting centre for the operations level provides control and oversight for the design and operation of risk solution operations actions, and determines whether actions require mandatory (as opposed to discretionary) implementation, in line with a risk assessment of risk severity and likelihood. It also monitors and evaluates all these operational risk features to ensure appropriate adaption and modification of actions and assessment to ensure ongoing effective risk mitigation.

At the business strategy level, Figure 5.5 shows the divisionally arranged business units’ DEs. These DEs are established and maintained by the application of the business strategy level injections, comprising the business risk library (Section 5.2.2.1), business actions (Section
5.2.2.2), business assessment (Section 5.2.2.3), business control centre (Section 5.2.2.4) and 
business monitoring and reporting centre (Section 5.2.2.5). This is where the monitoring and 
reporting centre, with business risk library support, implements business level contributions to 
maintaining appropriate risk appetite-related business unit behaviour. Appropriate risk 
mitigation actions are designed and operated across the business unit related risks (UDEs), and 
together, business risk assessment and control centre functions determine the effectiveness of 
the controls and make adaptive modifications where required.

At the corporate strategy level, Figure 5.5 shows the strategic injections (comprising risk 
appetite appropriateness (Section 5.2.3.1), cultural adaptation (Section 5.2.3.2) and the cross-
divisional collaboration centre (Section 5.2.3.3)) providing risk mitigation direction to the 
major strategic objective domains, comprising consumer business growth, corporate, small and 
medium business growth, wholesale business (product and market) growth and enterprise 
technology effectiveness.
Figure 5.5 Future reality tree injections mapped to financial institution structures
Importantly, the entire organisational view provided by Figure 5.5 also conveys that all the injection elements work together, directionally through the functional levels (operations, business and corporate strategy) and also cross-functionally and across the main divisional structures (demand in retail banking, supply in business banking, product management and enterprise technology). The results of the FRT analyses summarised in Figure 5.5 show that interconnectedness in risk control injections was found across the entire organisation. This potential future perspective (illustrated in Figure 5.5) was thought by the participants to offer the promise of more effective risk reduction than the current state described in Chapter 4. For example, Participant 2 explained:

*Whether it’s big IT, retail issues affecting customer satisfaction, risks with product development outsourcing, or just that they are so big and diverse, we have written off large amounts because the risk trade-offs are wrong. Because we didn’t understand properly. We need a system of controls that can get good intelligence about risks to make better decisions and to more effectively implement controls, I think that what you show here, reflects well how things should be in place ...*

### 5.4 Summary

This chapter first described the injections that the participants judged as needed to transform the current risk state into a desirable future state, where financial institution risks are effectively managed. Section 5.3 described the findings of the FRT analysis for each of the core problem areas, comprising demand in retail banking, supply in business banking, product management and IT. The FRT analyses interrogated and illustrated how the injection solutions would transform UDEs into DEs. Section 5.3.5 provided an entire organisational perspective of a
comprehensive and coordinated approach to managing financial institution risk. Next, the results from Chapters 4 and 5 are discussed in Chapter 6.
CHAPTER 6
DISCUSSION

6.1 Introduction

The findings presented in Chapters 4 and 5 on the nature of risk in the financial institutions investigated are discussed in this chapter. It first provides a summary of the approach adopted to answer the research questions in Section 6.2. Second, a summary of what was found is discussed in Section 6.3. The implementation into practice considerations of the research findings are described in Section 6.4, including how the findings could inform applied risk management in financial institutions that seek to transform a current state into a desired future state, such that UDEs of risk effects are transformed into DEs.

6.2 Summary of the research approach

This research conducted an exploratory investigation of the probable causes of FSCR common to Australian financial institutions, such that inquiry information from nine participants from three financial institution cases was aggregated into a single generic Australian financial intuition view of risk. The three financial institutions were sampled from three different Australian deposit-taking financial institution capitalisation tiers (large, medium and small), so as to be broadly representative of deposit-taking financial institutions in Australia (Gorajek & Turner 2010). Deposit-taking institutions are the largest financial institutions in Australia, and comprise banks, credit unions and building societies, which together make up about 60% of the Australian financial system’s assets (Donovan & Gorajek 2011). Life insurance companies and superannuation funds account for about a quarter of the system’s assets.
(2018) provides regulatory oversight of these parts of the Australian financial system. Australian deposit-taking institutions remained profitable during the global financial crisis, although they underwent changes where they strengthened their capital position and improved resilience by increasing the proportion of funding sourced from deposits and longer-term securities (Donovan & Gorajek 2011). While Australian financial institutions were therefore apparently successful in managing external risks, the questions in this research were limited to the internal organisational risks within the scope of more direct institutional risk control (Section 1.7).

To accommodate the complexity and multidetermined nature of risk causality in financial institutional settings, TP methods taken from the TOC (Goldratt & Cox 1984) management philosophy approach to organisational problem solving were used. The two TP methods employed were CRT analysis (described in Chapter 4) and FRT analysis (described in Chapter 5). These were selected to holistically examine both the contributing causes of the risks and the risk management solutions that could be applied in the future to control those risks (Kim, Mabin & Davies 2008). Unlike the typical thematic content analysis of case study data, which identifies and interprets themes (Braun & Clarke 2006; King, Horrocks & Brooks 2018; Vaismordi et al. 2016), TP methods instead seek to find the weak links within the firm that are significant and worth investigating, so that the issues that are found to constrain performance within the business can be overcome (Goldratt 2010). This includes the effects of any weak point or link within the organisation thought to radiate out to become a source of broader damage (Goldratt 2010).

The objectives of this research were, through the application of TP methods, to provide an in-depth understanding of FSCR and their mitigation in Australian financial institutions. An in-
depth understanding aimed to identify the nature and causes of FSCR in Australian financial institutions by taking an entire organisational view of FSCR from a supply chain perspective. A further aim was that this in-depth analysis could provide a basis to devise approaches for mitigating the identified FSCR appropriate for practical application in Australian financial institutions. The following research questions (RQ) were posed:

RQ1: What FSCR are identified as currently present in Australian financial institutions?

RQ2: What is the nature of the causal relationships among the FSCR that adversely affect financial institution business functions?

RQ3: What future risk control practices could mitigate FSCR in Australian financial institutions?

How these research questions were addressed to meet these objectives is described next.

To address the first research question (RQ1) about what FSCR are identified in Australian financial institutions, this research first developed a conceptual model of risk from the literature. The model included four main types of supply chain risk: inadequate demand management, supply management, product management and information management. Second, the model was applied, refined and developed through iterative interviewing inquiry with participants in a multi-case study design where the TP methods were derived from the TOC and where the cases were aggregated to provide a single, generic financial institution perspective encompassing the entire organisation. The participant informants were nine senior managers with risk management responsibilities from three Australian financial institutions.

Ho et al. (2015) suggested that the case study approach is an example of the types of methodologies needed to investigate associations among risks. Research that can use methods
that accommodate investigation among multiple risks, rather than in isolation, has potential to be used to make sense of real-world complexity in a way that informs practical risk mitigation models and understanding. The aggregated list of risks from the interview inquiries (see Appendix B) were interrogated and developed as part of the TP CRT method of inquiry used to address the second research question.

To address the second research question (RQ2) about the nature of the causal relationships among the FSCR identified that adversely affect financial institution business functions, CRT inquiry and analysis methods based on the TP methods were employed (Goldratt 1988; Kim, Mabin & Davies 2008); these have been extensively used both in research and applied to a broad range of organisational types and problems (e.g., Ikezeri et al. 2018), although rarely in financial institutions, and not with Australian financial institutions.

Originally developed from applied organisational problem solving (Rahman 1998), and suited to the nature of case study data (Kohli & Gupta 2010; Ikezeri et al. 2018; Mabin & Balderstone 1999), the TP methods accommodate the complexity of real-world application of organisation problem analysis and solving (Eisenhardt 1999). The methods used included the development of CRTs that model and map the multidetermined nature of problems (UDEs), to identify the main underlying causes from among a complex array of related, contributing and interacting financial institution risk effects (Dettmer 1997; Goldratt 1990). This method allows for multiple risks to be examined together, to determine their interrelationships from a holistic or entire organisational perspective.

The analysis of the contributing causes of undesirable risk was conducted at three organisational levels of the financial institutions. As described in Section 4.1, the first comprised the customer-facing operations level. The second, the business strategy level,
comprised the business unit functions of the institutional divisional structures. The third was the corporate strategy level that gives organisational strategic leadership for the achievement of organisational objectives and accountability to shareholders and regulators. This conceptualisation of functional structure was informed by the interview participants who formed a consensus view on Australian financial institutions that include banking as part of the financial services mix offered. This organisational modelling was undertaken to contextualise the results reported in Chapters 4 and 5, and served to illustrate the organisational location, nature and interrelationships of the core risks effects thought to be the key contributors to undesirable outcomes arising from FSCR.

The TP CRT method was applied to the core risk effects thought to cause UDEs in four main business areas of the financial institutions, applicable to each of the case studies, irrespective of capitalisation size. These four included demand-related retail divisions, supply in business-to-business relationships and transactions, the product development part of the business (which includes the development and management of financial products designed for resale through the wholesale market) and IT or enterprise services that electronically enable all the other services and critical financial functions and transactions.

To address the third research question (RQ3) about future risk control practices that could mitigate FSCR in Australian financial institutions, a future state analysis was undertaken. This examines the relationship between FSCR and the future application of risk treatments to improve risk handling. In this future state analysis, the results of the CRT analysis were used to develop FRTs, which model and map the application of proposed risk reduction solutions, called ‘injections’, in the TOC (Hohmann 2015). Intended to rectify the cause of problems revealed by the CRTs, injections are placed within the CRT map to illustrate and conceptually
test their effect, where UDEs and effects are transformed by the injections into DEs (Balderstone 1999). A FRT depicts the desired future, where the proposed injections are thought to effectively mitigate risk and resolve problems affecting institutional performance. The dynamic causal pathway mapping provided by both the CRT and FRT methods also provides for an examination of the entire organisation, where multiple risk determinants and mitigation are examined jointly. In this research, this gave a holistic perspective of a comprehensive and coordinated approach to assessing and managing financial institution risk, by mapping the desired future effects onto the entire organisation.

### 6.3 Summary of the findings

The findings provided a participant consensus depiction of the typical or generic Australian financial institution functions and organisational structures (Section 4.1). This served as a conceptual scaffolding to contextually illustrate the organisational functional location of the findings on the risks to be investigated (Chapter 4) and the risk solution injections to be subsequently developed (Chapter 5).

The participants’ views regarding the nature of the risks from a supply chain perspective in financial institutions were aligned and informed by the conceptual model of the four main risk types derived from the literature (Section 2.8), which, in turn, were also aligned to the major functions of the financial institutions. The use of TP CRT investigation methods with the participants provided for the consideration of multiple factors jointly, to provide a holistic approach to the examination of risk; this had previously been identified as a gap in the literature as supply chain risks had largely been examined in isolation rather than jointly (Fan & Stevenson 2018; Ghadge et al. 2012; Gelsomino et al. 2016; Ho et al. 2015).
A main finding was that the main types of underlying core risk effects contributing to these UDEs and hence corporate undesirable outcomes included people-centred failures, external service provider disruptions, policies and regulatory compliance limitations, and technology hub failures. These underlying core risk effect types and the UDEs that contribute to them are summarised Table 6.1 and Figure 6.1. For example, HR-related issues such as shortcomings in recruitment practices, insufficient in-service training, rigid procedures and lack of flexible policies to guide situational decision-making, were all undesirable risk effects labelled together under the core risk effect type ‘people-centred failures’. Similarly, the participants identified that many risks in product development and IT arise from poorly controlled risk, as functions are outsourced to contracted external service providers, which further contribute to risk in both retail and business-to-business banking. These underlying risks, although described as types, are not intended to be portrayed as exclusive of each other. Instead, all underlying risk effect types were found to constrain achievement in all four business areas, and contribute to retail banking failing to meet customer needs, business banking failing to meet targets, product management failures and IT disruptions. Further, the causal pathways associated with the core or underlying UDEs also cross over the functional levels of the financial institutions (operational level functions, business strategy level functions and corporate strategy level functions).

These findings align with the themes in the literature regarding the broad types of risk that have been described in attempts to create typologies of risk (Ho et al. 2015), such as demand, supply, product and IT factors, which formed the basis of the conceptual model described in Section 2.8. In the context of Australian financial institutions, these typologies or categories of risk made sense to the case study participants, who found that the model aligned with their understanding of banking business areas and risk. Further, rather than examining each type of
risk in isolation, this research collectively examined the internally controllable risk types, which were considered jointly to gain an understanding of their interacting effects in complex organisational dynamics. The results showed that the risk typologies were not mutually exclusive and had causal influences on each other. For example, people-centred failures contributed to both product management and technology failures. The results showed the interactive nature of the risk types—what the literature presented as arbitrary groupings of risk elements were found to be mutually bidirectional and cross-categorical in nature when examined dynamically with the TP CRT method.

In financial institutions, the interactivity found by the results among both risk types and organisational features also meant that categorising financial risk as separate from other kinds of risk is an artificial distinction in risk typology that has little meaning in an applied financial institution context. For example, previous definitions of financial risk have encompassed supply chain financing risk related to risk concerning adequate funding of supply chain activity (Popa 2013). Fan and Stevenson (2018) described a finance risk perspective related to accounting, working capital optimisation and asset financing. Popa (2013) also sought to make a distinction between general supply chain risks and financial risks. However, this research shows that all supply chain related risks in a financial institution have a financial aspect to them, regardless of whether the financial relatedness is direct or indirect. For example, people-centred failures can relate to financial knowledge and capabilities of people, adequacy of training in financial-related matters, or have financial impacts such as poor management of credit-related matters or failure to frame the financial aspects of external service provider contracts adequately. When examined jointly, rather than in isolation, and where a dynamic underlying causal pathway is mapped for the entire organisation, the distinction between FSCR and non-financial SCR previously made in the literature was not found in the results. These
findings support the more inclusive nature of the FSCR definition in this research, where it was defined as risk examined from a supply chain perspective in financial institutions.

As portrayed in detail in Chapter 4, Figure 6.1 shows a summary of the core risk contributing effects that were comprehensively mapped with CRT methods to produce what was seen as the current state of the institutional dynamics of FSCR in the financial institution cases under investigation. The CRTs illustrate an integrated and holistic view of the complex determinism of risk, taking account of the functional and structural characteristics of financial institutions identified in Section 4.2 and the nature of risk described in Section 4.3. Figure 6.1 shows how the results map onto the conceptual model described in Section 2.8, reflecting the grouping arrangement of the results on risk effects. The CRT results show that the core risk effects related to each of the four main financial institutions business divisions (demand in retail banking, IT, product management and supply in business banking). Figure 6.1 shows how the core risk effect types jointly contribute to FSCR in Australian financial institutions aggregated from the sample of the three financial institutions cases.
Figure 6.1 Summary of core risk effects contributing to FSCR
From the entire organisational perspective results described in Section 4.3.5, Table 4.5 and illustrated in Figure 4.7, Table 6.1 summarises UDEs found by the CRT analyses to make up the four main underlying core effect types that operate across financial institutions and contribute financial supply chain risk in the financial institutions. Building on the CRT findings described in Chapter 4 and summarised in Figure 6.1 and Table 6.1, the Chapter 5 future state analysis shows the results of FRT methods to provide a view of what the participants thought would be an effective and desired future, if these financial institutions’ underlying core risk effects were effectively managed. Solution options (termed ‘injections’ in TP) for organisational problems were identified and described over the three levels of major institutional functions (operations, business strategy and corporate strategy). The combination of injections working together across the organisation was intended to provide the overall solution to financial institution problems. The injections were mapped in FRT figures (Figures 5.1–5.4) for each of the four main risk domain areas (main businesses or divisions of the generic Australian financial institution): retail banking, business banking, product management and IT.
Table 6.1 Summary of undesired effects contributing to underlying core risk effect types

<table>
<thead>
<tr>
<th>Underlying core risk effect types</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>People-centred failures</strong></td>
</tr>
<tr>
<td>Inadequate staff training</td>
</tr>
<tr>
<td>Unfulfilled audit requirements (e.g., complaints)</td>
</tr>
<tr>
<td>Limited HR processes &amp; policies</td>
</tr>
<tr>
<td>Lack of specialised knowledge</td>
</tr>
<tr>
<td>Human data processing errors</td>
</tr>
<tr>
<td>Miscalculations</td>
</tr>
<tr>
<td>Poor recruitment process</td>
</tr>
<tr>
<td>Insufficient professional development</td>
</tr>
<tr>
<td><strong>External service provider disruptions</strong></td>
</tr>
<tr>
<td>Outsourcing issues</td>
</tr>
<tr>
<td>Business support disruptions</td>
</tr>
<tr>
<td>Frequent internal and external fraud</td>
</tr>
<tr>
<td>Communications and technology breakdowns</td>
</tr>
<tr>
<td>Lending operations discrepancies</td>
</tr>
<tr>
<td>Natural disaster (e.g., offshore business disruptions)</td>
</tr>
<tr>
<td><strong>Policy and regulatory compliance limitations</strong></td>
</tr>
<tr>
<td>Limited professional development and experience</td>
</tr>
<tr>
<td>Human error in database entry</td>
</tr>
<tr>
<td>Auditing issues</td>
</tr>
<tr>
<td>Government interventions</td>
</tr>
<tr>
<td>Regulatory non-compliance (APRA)</td>
</tr>
<tr>
<td>IT compliance requirements failure</td>
</tr>
<tr>
<td>Data security for Privacy Act concerns</td>
</tr>
<tr>
<td>Ethical and legal issues</td>
</tr>
<tr>
<td><strong>Technology hub failures</strong></td>
</tr>
<tr>
<td>IT system disruptions &amp; failures</td>
</tr>
<tr>
<td>Cyber security threats</td>
</tr>
<tr>
<td>EFTPOS &amp; ATM outages</td>
</tr>
<tr>
<td>Online banking outages</td>
</tr>
<tr>
<td>Business transaction disruptions</td>
</tr>
<tr>
<td>Application crashes</td>
</tr>
<tr>
<td>Communication and technology breakdown</td>
</tr>
</tbody>
</table>

As described in Chapter 5, the FRT method derived a consensus set of injections designed to be applied simultaneously at different levels, structures and functions of the generic financial institution. As summarised in Figure 6.2, the injections were intended to be mutually supporting, where the injections’ risk appetite, monitoring and performance centre, collaboration centre, libraries and risk registers all enable, guide and support the application
of the more directly intervening injections, comprising cultural adaption, control centres, business assessment and tactical actions.

The injections are envisioned to mitigate the UDEs of the core risk effect types, which manifest UDEs at multiple levels, structures and functions of the financial institution. The participants agreed that if risk was multidetermined in a complex organisational system, then to be effective at reducing risk, a risk mitigation approach would have to be comprehensive and comprise multiple cohesive components acting jointly as part of a highly organised approach to risk management and mitigation. An example of technology hub failure risk is where technology outages cause online, ATM and EFTPOS customer service failures. These can receive media attention because of their extensive disruptive effects on both personal and business banking (Graham 2018). A people-centred failure example was where the Commonwealth Bank underpaid about 8,000 staff after its HR technology systems failed to accurately calculate and process entitlements, forcing the bank to repay millions of dollars to current and former employees. This UDE example illustrates where a people-centred failure has a technology component (Australian Payroll Association 2019). Another example that attracted media attention was an undesired external service provider effect where a bank employee with responsibilities for external contractors was arrested for substantial fraud (Calderwood 2019).

Further, the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry showed that undesired regulatory compliance effects were found to be common in most major financial institutions in Australia (Commonwealth of Australia 2019). Figure 6.2 shows that the injections are conceived as risk management methods able to be applied to multiple core risk effects, regardless of type related to other people-centred failures, external service provider failures, policies and regulatory compliance limitations or technology hub failures.
The FRTs described in Chapter 5 illustrate how the participants thought that the injections could be used to neutralise the effects of the UDEs and convert them into DEs. Aligned with financial institutional functional and structural characteristics and levels, the organisational interfaces with the injections were linked with the core risk effect types, and included risk libraries, risk assessments and risk registers for people-centred failures, external service provider disruptions, policy and regulatory compliance limitations, and IT hub failures. Informed by the other injections, the control centres and monitoring and reporting centres provide control and oversight for the design and operation of risk solution actions and determine whether actions require mandatory (or discretionary) implementation via a risk assessment of severity and likelihood. The centres also monitor and evaluate all risk features to ensure appropriate adaption and modification of actions and assessment to ensure ongoing effective risk mitigation.

At the corporate strategy level, the strategic injections comprise risk appetite appropriateness, cultural adaption and a collaboration centre. These would provide risk mitigation direction to
the major strategic objective domains, comprising consumers, businesses (corporate, small and medium), wholesale (products and the market), and enterprise technology services. The amount and type of risk the financial institution is prepared to tolerate is called risk appetite (Reserve Bank of Australia 2018b). Risk appetite is influenced by core risk effects and the organisational system of interacting causal dynamics illustrated in the CRTs. A risk appetite injection indicates the risk policy settings at the corporate level at which the business can accept or reject risk vulnerability, and whether the related decisions facilitate or inhibit the attainment of organisational objectives.

Adapting risk appetite based on feedback loops from organisational intelligence provided by monitoring and reporting centres on changing risk attributes over time informs how an organisation articulates and updates its risk appetite and then communicates this to the organisation. Further, the risk appetite framework would inform the risk appetite statements that guide both internal requirements as well as what might need to be provided to regulatory authorities (Reserve Bank of Australia 2018b). These corporate strategy level injections provide entire organisation risk mitigation direction to the major strategic objective domains and business units and divisions, as well provide for the strengthening of cross-functional and cross-divisional collaboration to mitigate risk and to put in place the necessary organisational culture settings to support a risk mitigating context.

Fan and Stevenson’s (2018) review of supply chain risk management (see Section 2.6.1) identified four routinely cited elements (e.g., Hallikas et al. 2004) of supply chain risk management: risk identification, assessment, treatment and monitoring. Risk identification aims to discover all relevant risks and recognise future uncertainties. Fan and Stevenson (2018) found that risk types and categories vary according to the specific context under examination.
and that there was no agreed risk management typology. Risk assessment concerns identifying what constitutes risk, priorities for action, and assessment of the potential implications of taking action. Risk treatment was defined by Fan and Stevenson (2018) as having a focus on the categorisation of treatments and distinguished from mitigation, which was related to treatment implementation strategy, where different treatments might be matched to different risks to maximise mitigation effects. Also identified in the literature by Fan and Stevenson (2018), risk monitoring recognises that risk is not static, and monitoring for changes in risk provides for treatment strategies to be adjusted to take account of changes.

Table 6.2 shows the findings on all the injections identified in this research (Section 5.2) from the participant inquiries of the TP FRT method, conceptually mapped to the typology used by Fan and Stevenson (2018) in their systematic review of the supply chain risk management literature. In that review, they mapped the findings of over 300 papers covering multiple countries and industries.
Table 6.2 Classification of injections with supply chain risk management process typology

<table>
<thead>
<tr>
<th>SCRM Process Typology</th>
<th>Operations level injections (Section 5.2.1)</th>
<th>Business strategy level injections (Section 5.2.2)</th>
<th>Corporate strategy level injections (Section 5.2.3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk identification</td>
<td>Operations actions (Section 5.2.1.2)</td>
<td>Business risk library (Section 5.2.2.1)</td>
<td>Risk appetite (Section 5.2.3.1)</td>
</tr>
<tr>
<td>Risk assessment</td>
<td>Operations assessment (Section 5.2.1.2)</td>
<td>Business actions (Section 5.2.2.2)</td>
<td>Cultural adaptation (Section 5.2.3.2)</td>
</tr>
<tr>
<td>Risk treatment</td>
<td>Operations control centre (Section 5.2.1.3)</td>
<td>Business assessment (Section 5.2.2.3)</td>
<td>Collaboration centre (Section 5.2.3.3)</td>
</tr>
<tr>
<td>Risk monitoring</td>
<td>Operations risk register (Section 5.2.1.4)</td>
<td>Business control centre (Section 5.2.2.4)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Operations monitoring and reporting centre (Section 5.2.1.5)</td>
<td>Business monitoring and reporting centre (Section 5.2.2.5)</td>
<td></td>
</tr>
</tbody>
</table>

Operations level injections (Section 5.2.1)

- Operations actions (Section 5.2.1.2)
- Operations assessment (Section 5.2.1.2)
- Operations control centre (Section 5.2.1.3)
- Operations risk register (Section 5.2.1.4)
- Operations monitoring and reporting centre (Section 5.2.1.5)
- Operations risk library (Section 5.2.1.6)

Business strategy level injections (Section 5.2.2)

- Business risk library (Section 5.2.2.1)
- Business actions (Section 5.2.2.2)
- Business assessment (Section 5.2.2.3)
- Business control centre (Section 5.2.2.4)
- Business monitoring and reporting centre (Section 5.2.2.5)

Corporate strategy level injections (Section 5.2.3)

- Risk appetite (Section 5.2.3.1)
- Cultural adaptation (Section 5.2.3.2)
- Collaboration centre (Section 5.2.3.3)
Table 6.2 shows that a number of the injections operate in more than one risk management process category previously identified in the literature. For example, the corporate strategy sponsored collaboration centre operates across all the Fan and Stevenson (2018) categories shown in Table 6.2, as this injection concerns the cross-functional sharing of all types of risk information and cross-area collaboration on all aspects of risk management. However, Fan and Stevenson (2018) noted that the previous literature was limited regarding consideration of the joint effects and application of risk management. They reported that research has failed to identify inter-relationships between risk management categories, and noted Gange et al.’s (2012) observation that a holistic perspective was largely missing from the literature.

Importantly, the FRTs illustrate how all the injections are intended to work together, both cross-functionally and through the levels, to provide a comprehensive and coordinated approach to managing financial institution risk from an entire organisation perspective. This potential future perspective was thought by the participants to offer the promise of more effective risk reduction than the current reality. The participants were familiar with the individual injections or risk control practices, but the process of dynamically mapping them to remediate UDEs, together with seeing the multiplicity in risk causation revealed by the CRT findings, raised awareness about the effectiveness related to mutual dependency of the injections. In the validation phase, in which the FRTs were affirmed by the participants, they agreed that the injections should operate as a comprehensive and coordinated system of risk management that crosses all functional levels and business divisions, to maximise effectiveness. In Chapter 5, it was reported that the participants noted that organisational risk functions were often siloed (i.e., a system, process or business unit whose function is operationally treated as isolated from others), and that this functional isolation acts as a barrier
to effective risk mitigation. The solutions mapped in the FRTs illustrate the required connectivity between the injections.

The lack of examination of the joint effects of management risk identified by Fan and Stevenson (2018) and the examination of risks in isolation (Ho et al. 2015) reduces the usefulness of research in guiding the implementation of learning from research into practice. However, the perspective revealed by the findings in this research regarding the interconnectivity of injections and the attainment of a desired future was made visible through a holistic examination of both the current state and the future state that was accommodated by the use of TP CRT and FRT methods.

6.4 Implementation in practice

An objective of this research was to design strategies to manage risk that have potential for application in practice. This section discusses some of the considerations that the participants identified as concerned with the transition from a current state to a desired future state. This need for attention to implementation was illustrated by Participant 1, who reported that:

We want the big plan about how to apply all the risk reduction and control processes. What happens now where we might have similar things in place, is that each of these systems or processes at times starts looking like silos. So then developing silos, they become kind of quite obstinate about what needs to be done, how it needs to be done. There should be flexibility. There should be plans and guidance.

Figure 6.3 illustrates an example of a risk mitigation implementation process that could be employed to implement the FRT findings into the practices of a financial institution. It shows
how to transition from the existing organisational risk profile, informed by the CRT analysis, to an expected desirable future risk profile, informed by the FRT analysis, where the injections are implemented. The transition from the current state into a desired future state is illustrated in Figure 6.3, in which three potential phases of implementation are shown.

The first phase concerns the examination of risk as demonstrated through the CRT analysis. This provides the institutional intelligence about risk to inform the design and establish the risk strategies and frameworks to subsequently guide the implementation planning. These are informed by an assessment of risk, the formulation of an organisational risk profile, and the location and nature of risk aligned with the profile. This phase could be supported by methods such as the TP CRT. These are intended to show how the risk management strategy can contribute to and support the achievement of the financial institution service objectives.

The second phase is proposed to communicate the risk policies, comprising strategies and plans and other communication artefacts, to the organisation. Business units and divisions align their tactical or operational risk reduction strategies and plans with the organisation’s strategies and frameworks. One mechanism for this is a financial institution’s risk appetite statement, which considers the most significant risks to which a bank is exposed and provides an outline of the approach to managing these risks. All strategic plans and business plans for functional areas should be consistent with this statement (Reserve Bank of Australia 2018b).

The third phase is to implement the risk management approaches into practice, including the various injection solutions, supporting structures and functions. As described in Chapter 5 and shown in Figure 6.3, the injections include a collaboration centre, risk monitoring and control centres, risk assessment, and actions and a managerial process to continuously monitor and adapt. In summary, Figure 6.3 is an example of how a financial institution might transition
from a current state of risk to the implementation of a desired future state. Figure 6.3 illustrates how the findings of this research, or use of the methods demonstrated, could be utilised and implemented into the risk-related practices of a financial institution.

Going beyond the perceptive individual organisations, an implication of the findings is in relation to the insights gained from an entire organisation view that have been described. The adoption of this entire organisation view by the financial sector and regulators, could be inferred from the findings that there may be some merit in considering whether an entire organisation perspective and associated approaches to risk becomes integrated into sectorial policies or a risk appetite statement standards, where a whole of organisation perspective is required to be adopted.

6.5 Summary

In this study, the TOC methods employed provided for a more holistic view of supply chain risk (Gelsomino et al. 2016), both in terms of the CRT analyses (Chapter 4) that described the complex nature of existing risk, but also in formulating a risk reduction approach using FRT methods (Chapter 5) to guide real-world application in Australian financial institutions (Section 6.4). For example, Figure 6.3 shows how an approach informed by the CRT and FRT findings could be applied in an Australian financial institution. The national and regulatory context of Australian financial institutions was discussed, and the characteristics of the cases contributing to the generic Australian financial institution model that provided the context of the illustration of the findings were noted in Section 6.2.

This chapter summarised the research approach in Section 6.2; in Section 6.3, the findings from the analyses were discussed. They included formulating a generic financial institution
functional structure, describing the current state of the risk characteristics of the financial institutions (CRT), and formulating the injections to be applied to reduce risk and offer a desired future (FRT). Implications of the findings for research and theory, limitations of the research and suggestions for future research are discussed in the next chapter.
Figure 6.3 Institutional transition phases from a current state of risk to a desired future state
7.1 Introduction

The objectives of this research were to create an in-depth understanding of risk and risk mitigation in three Australian financial institutions, through an exploratory multi-case study approach using TOC TP methods. The purpose of this chapter is to summarise the findings, research implications, theoretical and practical contributions, and limitations of this research. This chapter is organised as follows., Section 7.2 revisits the research questions and explains the findings of this research. Section 7.3 discusses the theoretical implications and the practical application contribution of the research. Section 7.4 discusses the limitations. Finally, Section 7.5 discusses how this research could be extended in the future and Section 7.6 provides the concluding remarks.

7.2 Addressing the findings of the research

The objective of this research was to provide an in-depth understanding of FSCR and their mitigation in Australian financial institutions, to identify the nature and causes of FSCR by taking an organisational view of risk from a supply chain perspective in Australian financial institutions. A further aim was that this in-depth analysis provides a basis to devise approaches for mitigating the identified FSCR appropriate for practical application in financial institutions.

To fulfil these objectives, the following research questions (RQ) were posed:

RQ1: What FSCR are identified as currently present in Australian financial institutions?
RQ2: What is the nature of the causal relationships among the FSCR that adversely affect financial institution business functions?

RQ3: What future risk control practices could mitigate FSCR in Australian financial institutions?

To address the first research question (RQ1) concerning FSCR identified as currently present in Australian financial institutions, a conceptual model of risk was developed from the literature. The model included four main types of risk that the literature described as affecting institutional performance. These risk types relevant to financial institution services comprised demand management, supply management, product management and IT services provision. The model was applied, refined and mapped to the organisational characteristics. This was used to organise and make sense of the inquiries with participants. It was found that the identified risks were able to be aligned with financial instructional structures comprising demand in retail banking, supply in business banking, financial institution product management and enterprise technology. The risks identified were able to be mapped to these structures as well as to the financial institution’s functional levels, comprising the operations level, business strategy level and corporate strategy level.

To address the second research question (RQ2) about the nature of the causal relationships among the FSCR that adversely affect financial institution business functions, the risks or UDEs identified in answering the first question were examined by a TP CRT current state analysis. The underlying effect types that were found to affect the institution’s undesirable outcomes were people-centred failures, external service provider disruptions, policies and regulatory compliance limitations, and technology hub failures. These underlying risk effect types were found to constrain achievement in all four business risk areas, and contributed to retail banking failing to meet customer needs, business banking failing to meet targets, product management failures and IT disruptions.
The CRT method found that these causes of undesirable risk contributed at three organisational levels of financial institutions: a customer-facing operations level, a business strategy level (comprising the business unit functions in the institution’s divisional structures) and the corporate strategy level. This CRT modelling illustrated the nature and interrelationships of the core risks effects found to be the key contributors to undesirable outcomes arising from the FSCR identified. It was found that the risks are interconnected and their dynamic causal pathways crossed over risk categorisations, as well as traditional functional levels and institutional divisions.

The CRT method was applied to the core risk effects thought to cause the UDEs in four aspects of the banking businesses. These included the functions and divisions comprising demand in retail banking, supply in business banking, product development and IT. The risk effect types in these areas were considered jointly and their collective impact explored. It was found that all the risks had some financial relatedness, either directly or indirectly, in the financial institutional context. This included financial institution supply chain transactions, the nature of the financial products, the financial nature of information content managed by enterprise architecture, and both the financial content and impact of people-centred functions.

To address the third research question (RQ3) regarding future risk control practices that could mitigate FSCR in Australian financial institutions, the participants described a desired future state comprising a comprehensive risk management approach to inform the translation into applied practice in financial institutions. These were illustrated in FRT maps. The FRTs modelled the application of participant proposed solutions (called ‘injections’) to the problems previously identified in the CRT current state analysis. These comprised a range of risk remediation solutions operating across all three functional levels of the financial institutions, where a number of risk controls were proposed to apply to operations, business strategy and corporate strategy levels of organisational functions. A key finding was that, collectively, the
injections need to operate jointly and in a highly organised and managed system of risk management that dynamically adapts to intelligence and feedback about risk. This was considered essential for the effectiveness of risk controls as they change and evolve over time and in response to both the changing risk environment and gauging the effectiveness of the measures that seek to impose risk control.

7.3 Implications of the research

7.3.1 Theoretical research implications

This multi-case study and the findings of this research provided an in-depth understanding of the complex dynamics of supply chain risk in financial institutions. In a review of the literature, Ikeziri et al. (2018) lamented the lack of TOC research into supply chain risk. Kim, Mabin and Davies (2008) similarly noted that the focus of TOC research was often isolated, with limited apparent applicability to real-world organisations. The use of TP methods in this research facilitated a comprehensive examination of financial institution risk from a supply chain perspective that encompassed the entire organisational view. This novel approach comprised several elements that contribute to the theoretical understanding of financial institution risk. First, multiple risks were jointly identified and mapped together, giving an entire organisational view. Second, the relative importance of the risks for explaining business disruption was evaluated. Third, the interrelationships among the risks and the pathways of risk movement through the institutions was identified and the interconnected nature of risk processes demonstrated. These TP method elements, which Chapter 2 identified from the literature as showing potential, have through their application to financial supply chain risk in this research contributed to the better understanding of the nature of financial supply chain risk in financial institutions. Informed by this comprehensive examination of risk from a perspective that encompasses the entire organisation, the dependencies among risk
management phases and approaches that were demonstrated also contributed to better understanding of risk mitigation effectiveness.

Consequently, a major contribution of this research was to take a holistic approach that examines risks jointly rather than in isolation. It utilised the TP CRT and FRT methods in an approach that accommodated the complexity of an entire organisation perspective, and the practical application utility that such a perspective provides. The location and alignment of the CRT and FRT findings to an aggregated generic Australian financial institution structural and functional scaffolding provided a perspective to the findings that further showed the interconnectedness of both risk and the risk solutions considered. Further, these features of the research revealed the dynamic nature of risk causal pathways when risks are examined jointly and contextualised with organisational functional and structural characteristics. It also showed that distinctions between FSCR and other non-financial SCR when applied to Australian financial institutions are not readily separable. This is because of both the intrinsic financial nature of the business of financial institutions and the dynamic and interconnected nature of risk causal pathways.

A further limitation is that consideration of positive risks was outside the scope of this research. This is where a positive risk is any condition, event, occurrence or situation that provides a possible positive impact. The TP TOC methods employed only considered negative risks where UDE’s identified through the TP CRT method, were sought to model the conversion to DE’s through the application of the TP FRT method. This may be viewed as where identified UDE’s could be viewed as existing negative risks, are then examined as to how they might be converted to reduce negative impact and to potentially increase the likelihood of positive impact in a desired future. Examination of existing positive risk was incorporated into the methods, except in so far as participants may have drawn on their experience of risk management practices to inform their observations as part of the TP FRT method.
The research also sought to reduce the gap in terms of the lack of research on FSCR in financial institutions and to apply methods that can accommodate complexity and practical application utility. Further, it sought to fill gaps regarding risks that originate from internal organisational factors. Unlike external risks, such as financial system disruptions, where risk is indirectly managed through hedging or capitalisation strategies that seek to provide buffers against external stresses such as those experienced in the global financial crisis (e.g., Donovan & Gorajek 2011), internal risks are able to potentially be controlled directly. With novel application to financial institutions in Australia, this is the first study to apply TP methods from a supply chain perspective to undesired risk-related effects located within the institutions and able to potentially be controlled. It also provides a contribution where exploratory methods were used holistically to investigate, analyse and provide potential solutions to FSCR in financial institutions, where the variables under investigation were considered jointly from the perspective of the entire organisation rather than in isolation.

The objective of qualitative case study research, with an exploratory aim, is not to generalise to populations to the extent that a randomised representative survey might attempt, but rather to generate theory, which could be tested by other researchers in future studies or to take a confirmatory rather than exploratory approach in the methods employed (Al-Busaidi 2008; Eisenhardt 1989; Yin 2014, 2017). However, the multi-case sampling design used in this research is based on a case replication logic rather than a statistical logic (such as in a survey). The three cases were financial institutions representing one of three market capitalisation size tiers in the Australian financial institution system (Gorajek & Turner 2010). This was so the research questions were related to examination of FSCR in Australian financial institutions, rather than in any particular individual institutions with limited generalisability. The CRT and FRT analyses represented and were constructed from the combined data from all nine participants from all three cases aggregated into a single generic case. The nature of the
institutional cases was such that they are from the same industry sector rather than from different sectors. In addition, all the participants have roles related to the management of organisational risk. A multi-case study design comprising three financial institutional cases, stratified with three participants each to make a sample of nine participants, was thought to be a reasonable sample size to allow for the retention of the benefits of a case study design (Eisenhardt 1991). It also provided for a design benefit from the ability to cross-case triangulate and aggregate participant information, providing replicability across cases that gives increased generalisability over a single case (Patton 1999; Yin 2014). In addition, data volume was balanced with complexity to both provide an in-depth analysis typical of qualitative case methods combined with the facility to suggest generalisability beyond a single instance. These features of the design of the sampling were thought to provide a foundation to make observations about Australian financial institutions without the loss of depth inherent in larger samples using quantitative methods (Dubois & Araujo 2007).

In this research, the TOC TP CRT and FRT methods provided a thorough examination of risk variables considered jointly rather than in isolation, and provided for both risk identification and risk reduction possibilities. This demonstrated research utility where a holistic approach enabled a comprehensive examination of institutional risk from the perspective of the entire organisation. This showed that the TP methods have application potential to comprehensively identify, analyse and reduce risk in financial institutions.

The risks identified within the financial institutions were contextualised with the risk categorisations in the conceptual model aligned with both the literature and the financial institutions’ structures and organisational functional characteristics. However, unlike previous research where supply chain risks are often examined in isolation (Fan & Stevenson 2018; Ghadge et al. 2012; Gelsomino et al. 2016; Ho et al. 2015), this research used a current state method (TP CRT) applied to multiple risks jointly across the entire organisation, and found
that the nature of the risks are not easily separable into categories. An interpretation of the results is that a category-based approach would not take account of the mutual and dynamic connectivity between the risks demonstrated by the TP CRT findings. Further, the identified risks were found to be not singularly located in an isolated part or function of the organisations, but rather, their causal pathways spanned different functional levels and divisional structures. Where previous research has adopted a categorical approach to the examination of themes, this tends to create an artificial view that does not reveal the intra-organisational complex dynamics of the interconnectivity of risk. In the current states reported by the participants, there was a tendency for risk management components in practice to be isolated or separated from other components or restricted to business unit perceived responsibility boundaries. This observation is understandable in the context of the literature where approaches comprising the arbitrary categorisation of the examination of risk reflect previous researchers’ critiques of the literature (Fan & Stevenson 2018; Ghadge et al. 2012; Gelsomino et al. 2016; Ho et al. 2015) concerning the isolated rather than joint examination of risk. The findings show that both risk and the management of risk are likely highly interconnected, both among the risk effects, their causes and effects, and their mitigation (both the manifestation of risk and the mitigation of risk across organisational structural and functional boundaries). The findings lend support to calls for increased research attention on the importance of methods that can accommodate the examination of risk variables jointly.

In addition to the theoretical contributions facilitated by the application of the TP methods discussed earlier, the findings about risk interconnectivity from an entire organisation perspective also calls into question the validity of the categorisation of risk into financial and non-financial categories (e.g., Popa 2013). In the context of financial institutions, the findings suggest that this categorical distinction is not valid, as most risk examined from a supply chain perspective from a holistic, entire institution view is all either directly or indirectly financial.
in nature. The findings supported the inclusive definition of FSCR used in this research, which defined FSCR as risks examined from a supply chain perspective in financial institutions. This contribution can be extended to suggest interpretative caution in relation to the investigation of general supply chain risks where the methods employed are categorical in nature. Categorisation has the facility to reduce complexity as a way of helping to make sense of observed phenomena; however, an unintended consequence may be to convey an altered understanding that differs from the true interconnected nature of the reality of the phenomena under investigation, where the interconnections are not captured by the categories. This, in turn, may truncate consideration of the range of organisational effectiveness enhancement options available for implementation in practice.

7.3.2 Practical implications of the research

An objective of this research was to design strategies to manage risk that have potential for application in practice (Al-Busaidi 2008; Eisenhardt 1989). The findings of the CRT and FRT analyses extend understanding of the dynamics of financial institution risk, and show how they can be practically applied in a financial institution and give examples of the processes and risk-related artefacts that could be implemented. The findings show how the existing risk profile of an organisation (informed by CRT methods) can be transformed through a transition to a desired future state (informed by FRT methods). The implementation example in Figure 6.3 illustrated the phases to translate FRT findings to illustrate how the contribution to practice might be implemented.

The in-depth analysis comprising a whole-of-institutional perspective, where the findings were also mapped to a participant consensus view of generic financial institution structures and functions, both served to facilitate illustrating the practical applicability of the results and their interpretation. This was particularly so for showing that the nature of the underlying FSCR identified was not organisationally isolated or discretely located, but dynamically interacting
and affecting multiple areas, functions and other FSCR. The practical implication of both the current state and future state analyses is that organisations not only need to look at what individual risk control treatments they have in place, but ensure that they are interconnected in a highly coordinated and well-managed system of control, comprising feedback mechanisms and the capacity for adaptation that takes a whole-of-organisation perspective.

A broader consideration of the implications of the findings is in relation to the insights gained from an entire organisation view risk that could have benefits for the financial sector. Although outside the scope of this research, benefits regarding the adoption of an entire organisation perspective could be integrated into sectorial policies or a risk appetite statement standards, where a more systemic perspective is required to be adopted.

The major practical implication, therefore, is not so much about any particular risk or risk treatment; rather, it is the recognition of the high level of interconnectivity both in the nature of risk and the effectiveness of responses to risk. Many organisations may already have substantial risk control approaches in place; what this research suggests is that these, both in terms of their diagnostic and treatment functions, are best managed as a whole, as an interconnected system that transcends internal organisational boundaries that would normally govern the segmented and hierarchical organisation of work.

7.4 Limitations of the research

This research adopted two established TP methods (CRT and FRT) that evolved out of the TOC management philosophy and from practical application in manufacturing organisations (Rahman 1998). In Chapter 2, it was described how TOC and TP methods were later generalised and applied to many types of organisations and problem types. The interest in the approach was not only because of this practical problem-solving utility, but also because it could accommodate the complexity and multiplicity of determinants of organisational and
other problems that exist in the real world (Eisenhardt 1989). TOC has since been applied to many types of organisations and problem types (Ikezei et al. 2018).

The TP method can accommodate calls for greater use of organisational case study designs that seek a closer examination of associations among supply chain risk than what has occurred previously (Ho et al. 2015). In-depth inquiry and capacity to examine multiple variables and accommodate real-world complexity (Al-Busaidi 2008; Eisenhardt 1989) are the advantages of qualitative methods. The TP CRT and FRT methods are suited to case study designs, particularly as they aim to dynamically identify underlying causes and solution options (Kim, Mabin & Davies 2008). Despite these strengths, case study designs have limited representativeness and caution should be exercised regarding generalisability of the findings to other organisations (Yin 2014, 2017). In this research, this limitation was addressed to some extent by adopting a multi-case study design, where the cases were selected from different financial institution capitalisation tiers in Australia (Gorajek & Turner 2010) and then aggregated to a single generic case that was more generalisable than each of the contributing cases examined alone, because shortcomings such as lack of particular information in one case could be supplemented with information from another case. Similarly, a distortion in one case might be moderated by the information from other cases to present an aggregated case that is more valid than each of the contributing cases taken alone. With this case sampling and aggregation approach, the combined findings from the case were expected to be more likely to be representative and generalisable to other Australian financial institutions than if a single-case study design had been used.

Another limitation is the generalisability of the findings from deposit-taking institutions to other types of financial institutions such as insurance companies and other vendors of financial products. There is likely some similarity, as deposit-taking institutions also provide insurance products, but caution should be exercised in regard to confidence about making inferences
about comparability (Olsen 2007; Ruddy 2008; Välimaa 2008) due to variability in product and services mixes offered by the different instruction types. Another generalisability limitation might be between Australian financial institutions and those located in other countries. In favour of comparability is that some Australian institutions are global and some global banks operate in Australia, so many of their organisational characteristics are likely similar. Notwithstanding, however, in the Australian financial market, regulatory controls (APRA 2018) and other environmental factors (Donovan & Gorajek 2011) may differ from other countries. For example, core risk effect types that relate to the regulatory context may be less generalisable, but those relating to people-centred risk effects may be more generalisable.

One final limitation of this study is the possible bias that not only the researcher brings into the story, but the bias of each participant interviewed. Kvale (1996, p. 286) argued that ‘personal interaction in the interview may have a decisive impact on the results’. The researcher acknowledges that the TP inquiries, as a part of the research process described in Chapter 3, were reflected back to the participants for validation. The research also reflects the researcher’s implementation of the TP inquiry with the participants (Neuman 2014).

Through the recognition of these limitations, some of the results should perhaps be regarded as more suggestive than conclusive. Despite these limitations, this study makes a significant contribution to making sense of the complex dynamics of risk and potential risk mitigation approaches in financial institutions in Australia.

7.5 Implications for further research

In terms of future research, this study could be extended by further inquiring about FSCR and their management characteristics in a variety of other financial institutions, irrespective of whether banking service provision is part of the financial services mix or not. This would enable the researcher to further explore the theory and current findings with reference to other
cases where organisational and service characteristics vary from the cases used in this research. Whether similar results to those developed in this particular study were found, or whether the risk management practices of other such financial institutions may varyingly have similarities, could be examined.

As this was a qualitative study, the findings could be used to develop hypotheses, which could be examined using quantitative methods. For example, these could be tested by surveys, sampling a larger number of organisations. By utilising a quantitative approach, the design of such could be informed by the findings of this qualitative study. A larger sample of participants and institutions involved in the FSCR process could be approached in a confirmatory manner. Increasing the number of organisations and participants in future studies would enable an increased confidence in the generalisability of the results.

For example, while this study explored the risk characteristics of an aggregation of three financial institutions, it could be extended in several ways, including the investigation of the participants’ risk practices within other inbound and outbound parts of the supply chain process, which could be explored in more detail.

**7.6 Conclusion**

The management of FSCR in financial institutions was found to be important for organisational performance. FSCR were defined as financial institution risk effects viewed from a supply chain perspective that constrain attainment of institutional objectives. Chapter 1 of this thesis presented a brief description of the background of the research on FSCR in Australian financial institutions, the rationale for the research, the research aims and questions, and the research methodology used to meet the research objective.

Chapter 2 provided a review of the literature where supply chain risks, transactional risks and the impacts of financial risks to both global and Australian financial institutions were
discussed. Research on FSCR was then reviewed and approaches that have been described about the management of risks in the supply chain were examined. Based on the literature, a conceptual model was presented to describe the major types of risk components of the supply chain, including demand and supply operations, product management in the supply chain, and IT risk in the supply chain. The literature showed that the nature of supply chain risk is complex and multidetermined. The TP methods of the TOC management philosophy, previously applied in organisational problem-solving research, were shown to be able to accommodate the examination of multiple risks together.

Chapter 3 described the TP and qualitative methods to be used in the research process and the steps followed to meet the research aims, through the application of the adopted research strategy. First, the paradigm that formed the basis of the methodological framework and which was utilised to address the objective of this study was described. How the methodology would answer the research questions was explained and how the cases were sampled and the participants selected was described. Finally, the structure and design of participant semi-structured interviews, the CRT and FRT inquiry process, and ethical considerations were described.

Chapter 4 described the analysis and results of the current state analysis. It provided the findings of the application of the TP CRT method to interview data from senior risk management participants from three financial institutions. First, it described the nature of the function and structure of financial institutions in Australia. Second, it provided a description of the core risk effect categories thought to be the underlying causes of risk. Third, the findings of the CRT TP method over three functional levels of financial institutions (the operations level, business strategy level and corporate strategy level) were presented, to describe the contributions to risk and the proposed causal pathways among the risk-contributing characteristics at and between each level.
Chapter 5 described the analysis and results of the desired future state analysis. It provided the findings of the application of the TP FRT method, which proposed a number of solutions that jointly respond to the risks identified from the CRT in Chapter 4. The FRT findings showed what the participants considered a desired future, where risks are effectively controlled. Chapter 6 provided a summary of how the research questions were answered and a discussion of the findings, and how the findings could be implemented in practice.

This chapter summarised the research and the contribution of the findings to practical application, the research implications and the limitations. The TP methods employed were used to populate an entire organisation structural and functional conceptual scaffolding representing an aggregate view of the participating cases intended to give a generic view of Australian financial institutions comprising banking services. The TP methods accommodated the complexity and dynamic nature of both the causes of risk that affect institutional performance and the examination of the dynamic nature of a set of mutually dependant solutions.

This research was a novel application of TP methods from a supply chain perspective to examine risk and risk mitigation in Australian financial institutions. This research showed that an Australian financial institution perspective encompassing an entire organisation was accommodated by the application of TP methods. The theoretical implication is that rather than portraying risk arising from a discrete subset of variables and manifesting in isolation, the results revealed the complexity of supply chain risk determinism in Australian financial institutions, where risk causal pathways were found to be interconnected and crossed over organisational functions and structures. The results showed that the most influential risk core effect types comprised people-centred failures, external service provider disruptions, policy and regulatory compliance limitations, and technology hub failures.
The results also showed the causal risk pathways arising from these effects as risk moved dynamically among the operational level, business strategy level and corporate strategy level of the financial institutions and across the major business types comprising retail financial services, wholesale and business financial services, product management and enterprise IT services and management.

The findings contribute to extending understanding both of the nature of Australian financial institution risk and of its improved control through a similarly interconnected system of cross-institutional risk treatments managed as a whole. Consequently, risk mitigation implementation approaches in Australian financial institutions are recommended to be highly interconnected and comprehensively managed as an interacting and interconnected system of risk controls.
REFERENCES


Goldratt, EM 1990, *What is this thing called theory of constraints and how should it be implemented?*, North River Press, Croton-on-Hudson, NY.


Lawson, B, Cousins, PD, Handfield, RB & Petersen, KJ 2009, ‘Strategic purchasing, supply management practices and buyer performance improvement: An empirical study of UK


Leisyte, L 2007, ‘University governance and academic research’, *Case studies of research units in Dutch and English universities*, University of Twente, Enschede.


Lincoln, Y & Guba, E 1985, *Naturalistic inquiry*, Sage, Beverly Hills, USA.


<http://www.maxwell.lambda.ele.puc-rio.br/Busca_etds.Php>


Scotland, J 2012, ‘Exploring the philosophical underpinnings of research: Relating ontology and epistemology to the methodology and methods of the scientific, interpretive, and critical research paradigms’, English Language Teaching, vol. 5, no. 9, p. 9.


Yin, RK 2014, Case study research: Design and methods, 5th edn, Sage, Thousand Oaks, CA.


Appendix A: Semi-structured interview

schedule

1. Participant role description questions

a) What is your role in your organisation?

b) How long have you worked for your current organisation?

c) How long have you previously worked in a financial institution? and in a risk-related area?

d) What is your educational attainment?

2. Organisational characteristics questions

a) What are the main divisions or business areas (approximately 3 to 5) of your organisation and what is their principal business focus?

b) What are the main functional levels (same function across different business units) of the institution’s structure, for example, operational/business/corporate strategic levels?

3. Organisational structures validation/triangulation

a) Look at this draft diagram of a generic financial institution structure, does it fairly represent (in a generic way) the functions and structures in your organisation? What adjustments would you make?

4. Current state inquiry (Thinking process - What to change?)

Questions repeated for each of the four business areas/divisions and each of three organisational functional level consensus-agreed from (3) above:

- Three organisational functional levels comprising operations, business strategy and corporate strategy; and,
• **Four divisional/business functions retail, wholesale/business, product management, information technology management.**

a) What are the undesirable effects (UDEs) or risk effects from your perspective for each level of the organisation? (list undesirable effects & effects – not necessarily causes)

b) Does this risk effect really exist at this level and how do you know?

c) Is the UDE operation-business-corporate level located?

d) In what other ways is it undesirable?

e) Why do you/the financial institution tolerate the UDE/risk?

f) What institutional strategic objective/s is being constrained by the UDE?

g) What specifically results (if this... then…. what does it cause next?) from the UDE?

h) Is there a specific action/effect causes the UDE? (“Constraint”)

i) Are there other effects coming from this UDE/risk?

j) Are all the causes/constraints here equally responsible for a financial institution's performance? If not then which of the cause/constraints have the biggest effect?

k) Does this effect really exist in the current environment “How do we know this?”，“What about alternative explanations? E.g., Is it definitely lack of knowledge and not lack of time, or lack of motivation or some other factor?”

5. **Current state validation/triangulation**

a) Look at this draft diagram of UDE/risk effects mapped to each area of the generic financial institution structure, does it fairly represent (in a generic way) risk effects and their causes in your organisation? What adjustments would you make?

6. **Future state inquiry (Thinking process - what to change to and how?)**

_Repeated for each of four business area/division and each organisational functional level:_
Three organisational functional levels comprising operations, business strategy and corporate strategy; and,

Four divisional/business functions retail, wholesale/business, product management, information technology management.

Use current reality tree maps consensus agreed from (6) as interview stimulus exhibit

a) How we can mitigate the risk at the operations/business/corporate, what are your suggestions?

b) What is the institution’s strategic objectives (that the risk effects constrain and that we want to better achieve through more effective risk control?) (desired future)?

c) What are the critical success factors for achieving the desired future where the risks are better controlled and attainment of the institution’s objectives are less constrained by the risks?

d) What are the necessary conditions needed to bring about these critical success factors?

e) What (solutions/injections) would remediate the underlying UDE’s, how could the UDE’s be converted into more desired effects (DE’s)

f) Should a financial institution try and address all the causes/constraints”? What happens if it addresses only some of them?

g) Should a financial institution try to take all the actions or only a few of them? Which of them will have the most impact? Which action should be taken first, second and so on?

h) If several actions are being taken simultaneously, is there a way to know which of them is the most effective? Are there dependencies between the solutions, i.e., for one to work another must be also present?
i) How can a financial institution ensure that an action does not improve one aspect of the financial institution at the expense of another?

7. Future state validation/triangulation

a) Look at this draft diagram of injections and their effects in each area of the generic financial institution structure on each of the main UDE’s, does it fairly represent (in a generic way) how risk and UDE’s and constraints could be better managed in your organisation? What adjustments would you make?
Appendix B: Sample interview transcripts

Tier 1 Sample Interview

Researcher 00:01 Today I'm going to interview about the FSCR and this is part of my project for the PhD and post-graduate, post PhD as well. I'm going to start, Participant 6, to ask you a few questions. If there's a chance, to give me more information about what's happening in your organisation. Before I start to go in more detail about the project, can you tell me about what's your background in the financial institution and how many years you have been working there?

Researcher: 00:23 I want to put more details here. I just want to make sure I start recording. Recording now. Today we are going to be recording Tier 1 Participant. Tier 1 Participant: 00:25 For operational risk, so I have an operational risk lead. I don't have a credit risk means.

Researcher: 00:36 So Tier 1 Participant, I just want to ask you a few questions first and then I'll go into more detail about the demand operation and supply operation which are the most important things. Can you please tell me about background and your experience in the organisation?

Tier 1 Participant: 00:49 Okay. I joined the Bank in 2004. My first job was looking after the cash in transit contracts.

Researcher: 01:00 Oh, so

Tier 1 Participant: 01:03 We use **** predominantly.

Tier 1 Participant: 05:44 I worked in cash in transit. Then I worked in procurement more generally. Then I worked in operations. Then, for the last seven years I've worked in risk roles, including two years at ***.

Researcher: 06:05 When you talk about risk, which one?

Tier 1 Participant: 06:07 Operational risk.

Researcher: 06:08 Operational risk. When you say operation risk, what's involved?

Tier 1 Participant: 06:12 I worked in--are you familiar with the three lines of defence?

Researcher: 06:17 Yeah, first line second line.

Tier 1 Participant: 06:18 Yeah, so I worked in the second line team within the CRO teams in what was group business services. It's now in process and transformation, so basically supportive--

Researcher: 06:29 GBS.
Tier 1 Participant: 06:29 GBS. Yeah, that's right and I've supported lending businesses, the distribution businesses, financial crime when it was set up, broker business, so essentially the back offices businesses, not a customer facing business.

Researcher: 06:49 When you say about defence, you're challenging the first line?

Tier 1 Participant: 06:55 Correct so first line was responsible for managing risk.

Researcher: 06:58 Yeah, engaging with that.

Tier 1 Participant: 06:58 Second line was responsible for oversight challenge review of the work they did and the solutions and put in place and that's still the model we run today.

Researcher: 07:10 It is. I was looking to the model and how they are impacting because 2009 and now they have significant change about the structure.

Tier 1 Participant: 07:18 There's been significant change. The three lines of defence model has remained, it's slightly tweaked. When I started in risk, each business had risk people that worked together. Now they've been consolidated into what's called the management insurance function.

Researcher: 07:37 Exactly. What do you think about the second line defence? They should be working in the risk team or they should be working in the actual business unit? Or what about the first line and second line?

Tier 1 Participant: 07:48 First line should be in the business. It has to be in the business, has to be connected to the business, working with the business, sitting with the business.

Researcher: 07:54 Reporting to the business people?

Tier 1 Participant: 07:56 Reporting to the business because they need to be part of the business, otherwise the business outsources its first responsibilities to somebody else, so they need to have ownership and they need to have reporting line up. Second line needs to report to risk because they need to be independent, otherwise if they sit with the business, they have lunch with the business, they talk, they go for drinks with the business, you end up with a sceptic. It's very hard to maintain that level of independence if you're structurally aligned to who it is as you're overseeing. You need that separation, and you need to make sure that if you have a concern you can escalate it through a different chain of command.

Researcher: 08:38 Okay, so what do you think about—I'll come to that question later. This is your experience and anything change or what the change or the significant change has happened in the financial supply chain risk, in terms of operation, business banking, investment banking, wealth?

Tier 1 Participant: 09:01 I guess conduct and it has been a huge issue for this bank and I think it's an emerging issue for the Australian industry. There's more and more. There's a greater awareness with the new organisation of the risks we are exposed to based on the pavers of our people and the design of our products and initiative right through the supply chain. One of the ways BANK has tried to address that is by building special capability so that the products and markets business we have is a product design house.

Researcher: 09:40 Yes, part of their general design.
Tier 1 Participant: 09:42 That's right. The distribution business is a retail and business bank and distribution only, so they manage the risk of distributing the product, but they don't have any involvement in the design of the product. All product design is done essentially in one house in the products and markets area, so the risk teams that support their business have specialty expertise in there, whereas historically, within the retail business, we had both retail product design and retail distribution. That specialty was spread across.

Researcher: 10:10 Okay, the question is here--you said people that design the product and the people that deliver the product--when you design the product, you're not exactly the same person who delivers the product? What's the change they're facing or how you are going to improve the product? Because you have to implement the product in the market.

Tier 1 Participant: 10:26 The product design is responsible not only for the physical product, but also the process by which the product is distributed, so it's an end-to-end design requirement. Not only design the collateral that goes with it, in terms of conditions, all that sort of stuff, you're responsible for end-to-end design and then the distribution business basically just takes the product and sells a product as per the process.

Researcher: 10:50 Okay, because you answered the second question. That's why this is going to go through any change that has happened during that or

Tier 1 Participant: 10:58 That's probably doing the biggest from our organisation.

Researcher: 11:01 Yes, comparing with another bank--

Tier 1 Participant: 11:05 Yeah, and to be honest, APRA as a regulator struggles with that as a model because the other banks have regional models.

Researcher: 11:14 They take your information. They're taking your information.

Tier 1 Participant: 11:17 That's right. APRA can't quite get comfortable with, there's no personal 11:24 ?? for Australia. There's no one person that's responsible for end-to-end Australia because products and markets is responsible--element--the distribution business is responsible for the other piece, whereas your ends in model, bank1 model, the bank2 model--there was a hit of all Australia and they can go and say, "Tell me how you do XYZ in Australian." That's not way our model works, so we do have some challenges getting APRA as a regulator around the complexities of our model. Structurally, the other thing that's significant is we run a performance unit framework.

Researcher: 11:58 Yep. I know about that.

Tier 1 Participant: 12:00 That's right.

Researcher: 12:00 So what do you think, or what you have seen in the last decades in the banking industry? In the financial model, the business model. It's much more digital, right. Checks are practically disappeared. Cash is diminishing and--

Tier 1 Participant: 12:26 Yeah, Bitcoin

Researcher: 12:27 Yeah, well that that's an emerging technology, so that's right. The risks we face are much more around financial disruptions and tech companies, people who come up with PayPal-type disintermediation of the services that a typical bank like ours, we'd offer, but yeah. You know, it's around credit card transactions, just general penetration of credit
cards. The ability to not generate any sort of paperwork when a credit card service swipe; much more customer focused; online payments, mobile wallets, all that.

Researcher: 13:11 I want to ask you a question not from here. When you say about the credit card, why is the bank responsible for the credit card or any products? Why not the people that owe the organisation to produce the product.

Tier 1 Participant: 13:23 So Visa or MasterCard?


Tier 1 Participant: 13:27 Because what the banks offers is a distribution business, right?

Researcher: 13:30 Yep, different channel.

Tier 1 Participant: 13:30 That's right, yes. Visa are a global organisation, but in reality they're a quite small organisation, given the scope and reach because basically banks like ours are distribution houses for the visa card product.

Researcher: 13:47 Why they are not responsible the loss? For example, I have my credit card and I lost maybe 1,000-2,000, through fraud or whatever. Why the bank have the guarantee or they cover the loss? Why not Visa because they have produced the product?

Tier 1 Participant: 14:01 Because the bank–

Researcher: 14:02 Distribution, is the agent.

Tier 1 Participant: 14:04 That's right and part of the agency agreement is, for getting to clock the ticket on every transaction, I get to basically provide insurance or loss coverage to my customers for that. I have to make a trade-off.

Researcher: 14:21 Agreement.

Tier 1 Participant: 14:22 Business benefit.

Researcher: 14:23 So we're just contracting an agreement.

Tier 1 Participant: 14:25 That's exactly right.

Researcher: 14:25 Already you've done it with Armour Guard or Chop.

Tier 1 Participant: 14:27 Exactly, so it's the same sort of thing. I understand what my loss profile looks like. I get to manage and influence that because if Visa wore the final cost, they have no way of actually influencing the customer behaviour. They would then have to have huge numbers of staff to manage that. So if you lose your card, who are you going to ring? You ring your bank and because we manage the card, we will stop the transactions. We will also alert you proactively if we see some strange transactions on your card. If Visa had to do that globally for every card with their logo on it, that would just be unmanageable.

Researcher: 15:03 I understand that, but my other question is, I'm not asking Visa to manage that. I'm asking why we are not and putting some cost involved that if this client lost his card, like $1,000, say 95% the bank will cover that and 5% visa because that one will give the Visa the opportunity also to act in a proactive way to develop the new product that helps the bank.
Tier 1 Participant: 15:33 So you're arguing that Visa aren't incentivised to improve?

Researcher: 15:37 To making them improve their product,

Tier 1 Participant: 15:39 Yep, that's an arguable point, yes.

Researcher: 15:43 It's one way to they let them think about the way that they have to deliver a new product for you to innovate new things because when you ask them what is responsible, they will start to innovate something different, rather than just do the product and deliver it.

Tier 1 Participant: 15:57 Well, I think you'd have to argue that they have it right, so chip cards are a card manufacturer lead innovation that now exists that didn't exist twenty years ago. That wasn't made by a bank.

Tier 1 Participant: 16:09 Different product.

Researcher: 16:10 That's right. That was product development and certainly that has materially influenced the–certainly cardinal present transactions are more risky than when a card is present, so it has made a material difference and that's a product lead innovation.

Researcher: 16:27 So can you please explain for me the financial supply can work has worked in your organisation?

Tier 1 Participant: 16:34 That's where I need you to frame up some stuff for me and I will try and fill in the blanks.

Researcher: 16:38 Okay. Now, let's go to the personal banking–personal banking or go to retail banking, we call it. They have cash delivery for the branches and how it's work that, what's improvement or place or other way this. Other example like credit card when the customer go to the bank or customer going to deliver some money through their ATM machine, not through the branch staff.

Tier 1 Participant: 17:03 Okay, so we'd start a retail bank, so we have outsourced cash management, so cash services. They provide cash management services for all of our branches in Australia, so branches are on a delivery schedule and they get to–if they need special deliveries, whatever. Cash services, as you know, also manage our ATM deliveries and so they do all the tracking of ATMs and they do that.

Researcher: 17:30 AMC.

Tier 1 Participant: 17:32 Yep, that's right. Branches take deposits from ATMs, so for those ATMs that are in branch versus standalone ATMs, so they manage that and in emergencies branches can, not very often, but we'll stock ATMs, but typically that's done by–

Researcher: 17:56 Some of the ATMs, yeah. Very rare.

Tier 1 Participant: 17:58 For delivery of credit cards, that's often by customer preference and there's also a risk lens applied to that. There are certain suburbs that we would choose not to mail a credit card to a customer's home. We would ask them to nominate a branch and collect from this branch.

Researcher: 18:19 Based on what?
Based on crime stats, so western Sydney, for example, probably not so much.

Auburn.

That's right, you know the places, right? And southern Melbourne, so it's not a city centric thing, but there are certain suburbs where people can recognise what a blank envelope looks like and what it might be. They go through people's mails if mailboxes aren't secure.

Is that the government they have to put the different procedure in place to mitigate the crime or fraud?

I'm not sure it's necessary. Well, you should argue it's an overall government responsibility, but governments would see this as a bank risk. You are making money out of this product and the balance we need to find out is, to be perfectly honest, most customers, all customers, would prefer the credit cards delivered to their mailbox because it saves them a trip. We have to make a risk-based decision around how much we deliver on the customer’s wishes versus what it costs us when the card gets stolen and used for 48 hours.

Okay, but are you delivering the card, but you're not delivering the VIN number.

Yeah, but as know, it's got a chip.

Correct, but you can't activate the chip unless the customer calls.

But no, people that are good at that they can sell a blank card and then they can extract the information off it.

Which is they scan the device.

Its whole value to the criminal in society is a blank card, and it's not a great customer experience at the first--you know, you get a card and then it gets deactivated and then you have to fill out whole paperwork that says you didn't get the card. You state the date that says the card wasn't delivered. So that's credit cards. A lot of our wealth businesses is done through adviser channels. You asked about wealth, right, so we have some in-house advisors, but a lot of that was done by aligned financial planners and those sort of people

We know what's happening here, in UK, and other banks as well.

That's right and that's really a part of the challenging model. I mean, the advantage for us is it allows us to grow a distribution network really quickly. The challenge is it's how do we manage the quality of the service, the quality of advice, how do we make sure that the device is delivered, which is in the best interest of the customer and not necessarily the best interest in the adviser because there's always this internal conflict. If I sell you a product and I'm an advisor, I get paid for that.

Correct. Yes, you get commission.

That's right. Now, so I am challenged by if none of the products are suitable for you, what I should say is none of the products are suitable for you.
Researcher: 21:18 What about your performance?

Tier 1 Participant: 21:19 That's right, so there is an inherent conflict in that as a distribution model.

Researcher: 21:25 Exactly, that happened with bankA.

Tier 1 Participant: 21:27 With stock. That's right. Inappropriate advice was provided because the incentives were good. Certainly bankB has led the way with the reduction of commissions, so if you want a financial account from an email seat, that's alright, a financial plan for an email seat, you will have to pay a flat fee upfront and you clear what you're given and what you're not given and so you form a value about whether or not you want to invest another thousand bucks, 15 hundred bucks, whatever it is, to get a financial plan, but it's not commission based so advisors and senior advisors do a good job.

Researcher: 21:58 BankC first speak what happened in UK a few years back.

Tier 1 Participant: 22:03 Conduct losses, yeah. To a certain extent, we're a victim of the industry. Everyone was selling payment protection insurance. We are a very small fish in the Australian and everyone was doing the same thing and we were just a buff. Should we have been smarter on that? Yes, we should've.

Researcher: 22:24 Just more work.

Tier 1 Participant: 22:26 That's right.

Researcher: 22:26 What's an impact of the demand operation or the financial supply chain risk, when we're talking about demand.

Tier 1 Participant: 22:34 This is customs demand?


Tier 1 Participant: 22:35 Customers are more time poor so they have less appetite to meet in person. Things that can be done online digitally is good. The challenge for us on that is email legislation.

Researcher: 23:00 Yes, email, that's one of the things.

Tier 1 Participant: 23:02 Yeah. We need to be much–particularly around where there's a risk that we might be financing terrorists or accepting money from terrorists, we need to know the customer. The KYC requirements are much higher than they were and we need to make sure we've got an evidence-based defensible position. Now, to extent that you can create an identity online without ever going face-to-face, does represent a challenge. That's what the customer wants and for all the honest and genuine customers, that's a fantastic experience. The risk it creates for us is that we need a secure way of verifying that the person on the end of the phone line, on the end of the computer screen is the person they're portraying to be and that's the risk for us.

Researcher: 23:56 Okay, I like that. When the customer come to the branch or engaging with the bank, why not create a new account or new email?

Tier 1 Participant: 24:10 Like a bank generated email?
Researcher: 24:12 Yeah, which is easy, more secure.

Tier 1 Participant: 24:16 Yeah, absolutely, so when we have email correspondence or we have message correspondence within our internet banking, offering.

Researcher: 24:22 Yeah, I was thinking that's why the bank is one of the worst transactions. Create account.

Tier 1 Participant: 24:28 But you're a customer. If you want to be communicated to–I mean, I don't know about you, but I have three email accounts. I don't actually want a fourth one that's a bank one. What I want is for the bank to communicate with me with the email accounts I currently use. If they want to send to me–your statements are available–I want that to my existing email account. I don't want to have to remember to go into my internet banking to get a message or I'm already in my internet banking–I can see my statements are there.

Researcher: 24:59 Yeah, but the email more secure.

Tier 1 Participant: 25:03 The email is more secure.

Researcher: 25:05 One thing. The other thing is like you can generally, like how you have credit card, exactly how you have to have your email. You have your online banking, but you have your own email. They've logged everything what you want, checking all the history. Instead of sending invoices, invoices, or sending envelopes or bank statement transactions.

Tier 1 Participant: 25:24 Absolutely by preference, we don't mail anything to any customer. We would like all customers to deliver–they can get electronic copies of the mortgage documents, they can get electronic statements that are online, are archived for seven years. They can generate all their tax statements online, so all of that is the way the customer, so they can do all their banking from home. That that's what they want because they don't want to have to A find a park outside of a city branch, go into a branch, wait in a queue.

Researcher: 25:56 No parking.

Tier 1 Participant: 25:57 But also, I mean they're prepared to do that, if there's an advice or if there's a specialist element to the conversation. But if it's just I want to get a credit card, I want to get a form, I want to I want to get a statement, they don't see that as value adding for their time. They can have that delivered to them.

Researcher: 26:16 Yeah, that's correct. How are we going to minimise that–the demand operations challenge?

Tier 1 Participant: 26:27 It's always going to be a trade-off between making it as simple as possible for the genuine customers.

Researcher: 26:37 Simplifying them.

Tier 1 Participant: 26:39 Simplifying the whole process, so getting on-boarded. One of the challenges for us, and maybe it's the same for other banks, but certainly for us is that if you charge through multiple channels, and multiple systems won't talk to one another. If you're an MLC customer and then you open and join a–you get a transaction account and maybe you've come to a talk with business banking, you get a business account, you will probably end up with three different profiles.
Researcher: 27:12 What about the complexity here?

Tier 1 Participant: 27:13 That's the trade-off. We have vast number dollars invested in complex systems. Aspirationally, what we would like to have is a centralised customer management process.

Researcher: 27:25 Next gen?
Tier 1 Participant: 27:26 Next gen will go some way to that, but essentially that's still a personal banking platform. It's certainly not in the life business so ZZZ products, insurance products won't sit there in generation one. It's not a business banking platform at the present time. In an ideal world, customers expect because I've interacted with you once that you know who I am and that I don't have to repeat everything. Now, that's a reasonable expectation of the customer. It's very hard to do from a technology and multiple systems point of view.

Researcher: 28:00 It's theoretically easy to draw.

Tier 1 Participant: 28:04 It's easy to draw, exactly. That's right.

Researcher: 28:04 But to implement it in reality it's a lot of thinking, interactions, especially when you put in the customer with the business, with the internal, with the external, provider services, internal provider, operation, and all that. Integration is not easy, especially when—because I have IT background, I understand how they're engaging interaction between all the application, how they talk with each other. So it's not easy to implement the theory there and that's in programming language. It's very something very complicated.

Tier 1 Participant: 28:31 That's right, yes, and the reality is even if we had a centralised thing, how much information do we collect on the very first time we touch it because if it's just a credit card, you just want name and address and confirm your identity and they'll let you go, but if then you want a transaction, then we'd need more information, right? So do we collect all that information the first time you touch us? So there's always that trade-off between what's the right customer experience, what makes sense for us to deliver as a bank, and how do we make sure we're managing the risk?

Researcher: 29:02 Privacy you're talking about?

Tier 1 Participant: 29:04 Well, privacy is one issue, but more importantly how do we make sure we're managing the AML risk and the serious financing risk because that also, particularly since modern place and ISIS is sort—all of that sort of stuff—we are getting a much stronger focus from a Austrac around how robust our process is. They don't care about customer experience.

Researcher: 29:31 No, no, they don't care.

Tier 1 Participant: 29:33 They want to make sure that every person that comes in the door we've done an appropriate level of identification. So small business customers, they close their shop at ten o'clock. They want a channel that allows them to deposit cash at night, so we have an ATM that'll take a deposit.

Researcher: 29:48 That's exactly what I'm looking. The other question is what are the impacts of the supply operation? We spoke about the demand. Now we're talking about the supply operation.
Tier 1 Participant: 29:58 Well, supply is we need to find ways to have more customer friendly interfaces, so banks are now open on Saturdays. Ten years ago, twenty years ago that never happened. Banks were open from nine used to shut at five, maybe four on Friday, so all that. ATMs do a lot more than they used to do. The ability to make a deposit, to bank a check—all of that sort of things outside of ours. There are more ATMs. ATMs are smarter.

Researcher: 30:27 2,000.

Tier 1 Participant: 30:27 That's exactly right, so all of those sorts of. We're increasing touchpoints in shopping centres, we're experimenting the sort of advice-based kiosk type stuff. What we're trying to do is rather than force the customer to come to us is to have our points of presence where the customer is already there doing something else.

Researcher: 30:49 So you mean enhancing the relationship between the bank and the community or the customer?

Tier 1 Participant: 30:55 In the customer, yeah, but the old banking model was we decided based on—we would get a whole lot of space on a high street and we'd build a great big branch there. Now, they're getting smaller and because we actively discourage people to go for a branch for a lot of stuff that used to have to go to a branch for now. So we're actually trying to say you should be able to most of what you need to do with us online and if you can't, we'll try and put somewhere close to you on a Saturday.

Researcher: 31:28 That's really good. What about in terms of the supply contractor like ****************** what they have, the application.

Tier 1 Participant: 31:41 Yeah, so our demands of them are changing to. One is I think we're moving to stronger partnerships, so we're looking to leverage their expertise from other clients and also other industries. I think part of that problem—

Tier 1 Participant: 32:01 That's really good points because came to the Visa card because when I said to you, "We have to make them responsible 5% or some percent do that." They're focusing on not only just to deliver the product or the bank, they're focusing to innovate a new way to enhance and lift the bank's performance because as a supplier for the service they have not only just to do the business, they have to help the business to move forward. It's not going just to bring the card, it's they have to innovate a new way. It could be something small—chips; it could be something on the phone; it could be something different; it could be like using like different technology. Our life is evolving and changing very quickly and we have to be more strategic focused and fast and fast innovators. Other than that, we will be left behind and we'll never meet what's the market needs because our life is changing. Since 2000 and now, a huge change, so we are able to adopt a new thing is the thing.

Tier 1 Participant: 32:56 Thirty years ago, the only fun you had was in your house and it was tied to the wall.

Researcher: 33:02 Overseas nothing.

Tier 1 Participant: 33:03 That's right. Now if you walk out without your phone or leave your phone at home, it's like your arm's been chopped off.

Researcher: 33:09 Yeah, you can't live.
Tier 1 Participant: 33:13 That's right and people are used to being able to do things on the phone. They can look up stuff on the phone, they can book stuff on the phone. They expect to be able to pay for stuff from their phone. They expect to be able to use their phone and not have to carry a wallet.

Researcher: 33:24 Do you have any measurement in place to measure the risk that you have?

Tier 1 Participant: 33:29 The risk, yes. We quantify risk.

Researcher: 33:30 Based on what?

Tier 1 Participant: 33:33 Operational risk by capital, so we have a capital model that my team runs that's based on inputs that around our internal loss history. We have some future looking lost scenarios. We also take we also buy external loss data from all over the world. ORX. And we use another internal scoring mechanism that basically rates all of our PUs about how mature they are in their risk management.

Researcher: 34:07 Which application are you using?

Tier 1 Participant: 34:09 We've just implemented. The model is a home built model, a BANK built model. The Oracle platform we've introduced, risk map, provides the internal loss data.

Researcher: 34:19 I recognise 12 I.

Tier 1 Participant: 34:21 That's an Offša product.

Researcher: 34:24 Have you heard about SAP Financial Friendly risk?

Tier 1 Participant: 34:31 No, is it good?

Researcher: 34:32 I recently had a discussion with one of the directors there, guy from my– when I was working for and he said it's a new product for the banking and the banking going to like something different. I spoke with him a next gen. He said it is very complicated and I think they will face a lot of difficulties to implement it, reality. So I said maybe.

Tier 1 Participant: 34:58 I think all big systems you have a little bit degree–

Researcher: 35:01 Everything, exactly.

Tier 1 Participant: 35:02 We use **** for our HR records. Operational capital, that actually calculates at a hollow bank level what the appropriate level of capital we need to hold to manage our risk. We also measure losses and record losses. Businesses will plan and have a financial plan so they will measure their performance against how much they've had to put away versus how much they expected to lose.

Researcher: 35:26 That's when 35:27 Var and Non-Var, something like that?

Tier 1 Participant: 35:29 Yeah, so on a market risk basis, that's right. For operational risk it's just a non-lending loss plan line.

Researcher: 35:36 Okay the other question is information system management. What are the impacts? You touch it in the some over here about information privacy.
Tier 1 Participant: 35:48 And it touches everything.

Researcher: 35:52 Data governance, data integration, monitoring, outsourcing, communication.

Tier 1 Participant: 35:55 So that's one of our big risks good that if one of the new things is that we probably haven't paid enough attention to how valuable our data is and how accurate we need it to be. So things like keeping up-to-date with people's email addresses you keeping up-to-date. That stuff is really hard because there are some documents that we required by law or where we don't have customers consent to send it by email. We have to physically distribute and then we get a third, 20% back because customers have moved. And that's just a cost and a waste to the organisation when the customer doesn't get the information they need or require.

Researcher: 36:49 Instead of that they're moving, so about the email they can check emails.

Tier 1 Participant: 36:54 The email moves with them, so that's great. I have the same email address I had 10 years ago or 15 years ago. But I'm at two different addresses in that time.

Researcher: 37:08 Exactly. What you're saying is there's a right way and a correct way. Why Australian provost they're implementing they force everyone to have email and why not the bank?

Tier 1 Participant: 37:19 Two reasons for that. We would love to get customers to have email.

Researcher: 37:24 Yes, like have your customer come to the branch and you have to provide email. They'll provide ID, they have to take their email.

Tier 1 Participant: 37:31 And that will happen over a period of time, but for a certain generation of customers, perhaps slightly older than me–

Researcher: 37:42 That's still young.

Tier 1 Participant: 37:43 Yeah, but they aren't comfortable. They don't trust email. They have a level of concern around being able to do that. And also they like–


Tier 1 Participant: 37:58 They do. They like to walk into a branch once a week and say hi to Mary who's behind the thing and Mary knows them and they'll have a five minute chat and that's why the queues are so long, that customer loves that interaction.

Researcher: 38:09 Social.

Tier 1 Participant: 38:11 That's right. Whereas, I would choose never to go into a branch if I could and it's not that I don't like branch people, it's just that–

Researcher: 38:18 People difference.

Tier 1 Participant: 38:19 That's right. I'm a busy person there's no value for me going into branch. I mean, it's a little bit simpler given that I have to walk past a branch to go into the building. So if I have to I can, but my choice I'm never going to go. Anyway, we're talking
about technology systems. The challenges that banks historically have had large, big, monolithic, centrally run technology systems which are incredibly hard to maintain, incredibly hard to update large amounts of investment that require multiple years of delivery to do. That's not the customer's experience when they can get a new app in three seconds right and if they don't like that app they'll go and try another one. So that's part of the challenge we're facing is that we have a business model that's based around having central, everyone access to the data and customers are used to providing their data to 25 different apps, but that each of those apps are something very unique, very specific, and very value adding for the customer, and that's the challenge we are facing.

Researcher: 39:24 What about the processing and the payment?

Tier 1 Participant: 39:26 Processing the payment? That probably hasn't changed as much as other parts of the bank. It's still banks settling with each other that still. Even though a customer may do it via internet banking, once it gets to us it's still essentially processed the same way. If it falls out, it's still recovered the same way or a customer inquiry, so that part I mean there's probably some on the trade area where it's gone from it used to be all paper docks. It's now gone to digital, but fundamentally that part hasn't changed for the big banks. I guess where it becomes challenging is you get people like PayPal and bitcoins and these sort of things. PayPal less so because at the end of the day there's a bank at the end of the transaction.

Researcher: 40:20 Yes, now, that's very good point.

Tier 1 Participant: 40:21 Bitcoin is very different, right, because there isn't a bank at the end of that transaction.

Researcher: 40:25 Now why we are not using why we are using PayPal? We're not using the bank, or a credit card? Because if your PayPal account doesn't work you can use your credit card.

Tier 1 Participant: 40:38 That's right.

Researcher: 40:38 So why we are duplicating our process?

Tier 1 Participant: 40:42 I don't know, but there must there must be something that customers--and PayPal I think quite quickly worked on two things. There's general customer fear about providing their credit card on an Internet transaction.

Researcher: 41:00 Directly to their client?

Tier 1 Participant: 41:01 That's right, yep, and so they said we can have a we can make a position here, we can make a market here that says will provide a certain level of security for both the buyer and the seller -

Researcher: 41:12 Correct.

Tier 1 Participant: 41:12 And we will clip the ticket for doing it

Researcher: 41:15 But even when we do that through the credit card then it's going only binary digits, so how they are another end going to know that?

Tier 1 Participant: 41:23 No that's right yeah.
Researcher: 41:22 So same thing duplicating the process.

Tier 1 Participant: 41:24 It is, but they've been able to convince customers that there's value that they provide in their transaction.

Researcher: 41:33 That's one of the good things. What do you think about if there is anything that we are going to eliminate or minimise the risk that involves information system or information system of the information management, information system of technology system, application, hardware, software contracts as well?

Tier 1 Participant: 41:57 We will minimise some of the physical risk through cloud-based storages and virtualisation of storage, so we will no longer be exposed to a sprinkler going off and hosing down, right? That doesn't happen anymore so I think the physical risk, the robustness of the systems is going to be there. However, we are more exposed to cyber threat

Researcher: 42:26 Cyber, yup, technology.

Tier 1 Participant: 42:26 Yep absolutely and there are people who make a living out of trying to hack banks and they're very good at it and certainly we expect it. It's not an if, it's a when it will happen. So we invest a lot of money, time, and resources

Researcher: 42:46 Integration, security level, encryption.

Tier 1 Participant: 42:49 Yeah both security, but also in detection and being able to shut it down as quickly as possible

Researcher: 42:54 We face that skimming device, internet banking, especially internal could be the challenge that we face, especially if we remember in 2011 when the ATM used to double digit, give money. Last week or two weeks ago, one bank in India lost a huge amount of money through their cybersecurity, a huge amount of money

Tier 1 Participant: 43:21 Yeah it's happening, it's coming right. The other thing is we need to educate customers about the risks right because what's a really bad customer experiences is if I get a lead of an email potentially from a bank and it says look we're about to lock you out of the system you just need to confirm that you are still a valid customer, unfortunately there's a reasonably high percentage of our customers that will click on that link, provide their security details, and think they're doing the right thing. Now, at the end of the day we're probably going to make good on that to the customer although we have no legal requirement to. From a customer experience point of view we've got to make good on that.

Researcher: 44:00 The question is, what are the impact of the product management and also the challenge that they're facing and how we are going to minimise the risk when you talk about the new product life cycle innovation and other things?

Tier 1 Participant: 44:13 Okay so products are no longer designed for 5 or 10 years horizons; they're designed for one or two so there's a much–

Researcher: 44:21 Mainframe.

Tier 1 Participant: 44:21 Yeah there's a much faster expectation of product design, get it to market quickly.

Researcher: 44:29 Or respond to market need
Tier 1 Participant: 44:30 Respond to market need, get it in there, and we talk in the bank about file fast so MVP, Minimum Viable Product. Have an idea and get it to the market as quickly as you can. Test of a customer and say, "Hey, look, 80% of this is good. This is the 20% you need to." Fix that get it out again, so that's an agile delivery, but also an expectation that that product is probably not going to be around over the next ten years. You need to continually have new products coming along that meeting new needs of customers, so the idea of a single transaction account that does all the customers, which is the way we traditionally design for a bank, doesn't exist anymore. It's also around you know how can we deliver it to the customer in the way they want receive it, so whether that be via phone, via internet banking and what’s the trade-off between usability functionality and risk.

Researcher: 45:29 What's the risk involved?

Tier 1 Participant: 45:29 Well the risk is if you lose your phone and you haven't locked it, people can access or people in steal your identity so identity theft applies. We get people calling our call centres saying you know, "I'm Tier 1 Participant. I've lost, my house has burned down," but you know whatever, trying to steal my identity and then move money around. So it's that always that trade-off between what's the experience you want to give 99.9% of your customers who are doing the right thing and are genuine versus mitigating the risk of the .1% who are there to try and damage the bank.

Researcher: 46:06 Sorry for interrupting you because I think time running out. What KPI involved in your organisation?

Tier 1 Participant: 46:13 We use KPIs at a business level so PU or performance units, whatever a standard set of KPIs.

Researcher: 46:18 PU?

Tier 1 Participant: 46:20 Performance unit. Within risk, we have KRI's, we have key risk indicators by product, by process that help identify with the product price is within its bounds.

Researcher: 46:36 That's one. And what's the bank percentage that they put in for performance and risk.

Tier 1 Participant: 46:41 So we basically track that against how much money we're losing versus how much we expect to lose.


Tier 1 Participant: 46:47 Now that we've sold the UK our numbers look a whole lot better. So we're tracking better than last year, but things like card fraud, cyber fraud–they go up and down depending on you know, who's winning the battle whether the banks and the card companies have been able to lock it down or as soon as something's discovered you know they just hit you up well fine.

Researcher: 47:09 Yeah what's the relationship between the financials supply chain risk, what we're talking about and then the performance of the organisation? We spoke about all the difference.

Tier 1 Participant: 47:22 Well I mean you've looked at our financial reports. The largest write-offs we've had have been related to risks, particularly in the UK. We've written off
large amounts so if we get the risk management trade-off wrong, if we are exposed to risks that we didn't understand, we end up impacting the financial performance significantly. For credit risk and those risk, those are those are cyclical and we follow the market up and down and the margin tends to flow with that, but for operational risks, it's not a flat thing so conduct risk blows up and then it comes down again, and then cyber risk or fraud or–there is no cyclical pattern and there's no way you can build those prices in. So it's very much an exposure model.

Researcher: 48:13 Okay, so that means that there's a significant relationship between the financial supply chain risk and the performance for the bank. Is that one a positive thing or negative thing?

Tier 1 Participant: 48:23 Well, if the risks increased, it's negative for the performance of the organisation, yeah. I guess the point I was trying to make, there are no leap–so when we start losing money on a credit cycle, we start increasing interest rates to reflect that. That's not an acceptable response when we start losing money because of operational risks. So if we're exposed to more fraud we don't up the credit card rate on all our customers, right. You can't do that.

Researcher: 48:53 Do you have implement any technology or money theory in a place to minimise that the risk that the bank they are facing, such as Six Sigma, Kaizen, or other?

Tier 1 Participant: 49:03 So yes so this is quite a strong Kaizen implement that we focus a lot around process improvement. Is it focused particularly around risk? No, but it is focused around trying to make the processes robust, resilient, and repeatable, and so to a certain extent that reduces the risk of the process but it's not driven with risk as a focus. There's acknowledgement that risk as a positive outcome, but typically it's driven around what is the customer experience and how do we make it? How to reduce errors in the process so for the customer it's right first time 100% of the time? So the focus of tends to be more around customer experience, yeah.

Researcher: 49:43 Do you think that the relationship between relationship between financial supply chain risk and the performance of the bank can be enhanced in a positive way by Kaizen or Six Sigma or other theory?

Tier 1 Participant: 49:53 Absolutely. If our ability to minimise--well given I've said there's a link between how much money we're losing and financial performance, we can improve how much money we lose by improving the processes and the risks. So yes, whatever the tool is--Kaizen, Six Sigma--yes.

Researcher: 50:10 Yeah, I doubt Six Sigma is one of the process

Tier 1 Participant: 50:14 I'm less fussed on what the tool is, but if you focus on mitigating the risk, the challenge always is that you can lock the bank down and reduce your risk, and then you've got no customers left right? So it's what is the risk reward and to a certain extent, banks are in the business of taking risk. That's what we do, that's how we make money. And as a consequence, we're always going to lose some money. It's getting the balance right between customer trade-off and minimising your risk.

Researcher: 50:46 One of the last questions. What about the development staff and training and all those things? Any specific training or just knowledge-based or this requirement to read?
Tier 1 Participant: 50:58 So yeah, so we have–within risk we have–we have three levels of risk training that all the staff are required to do depending on the role. We have general information security training that all staff are required to do.

Researcher: 51:15 Compliance.

Tier 1 Participant: 51:15 That's right so there are–and that's refreshed on an annual basis. So you know there's training around health and safety, so managing people risk, mental health risk–so there are various training courses that are required of all staff. And then for people in specialist roles there's specialist training so the cyber security guys will do different training.

Researcher: 51:40 So what do you think what the way the best way to or what's your suggestion to mitigate the risk that the bank facing now? General question.

Tier 1 Participant: 51:47 General question?

Researcher: 51:49 Because I'm going to use this question to implement a new strategy, especially you see the complex relationship between all the business units.

Tier 1 Participant: 51:57 So I think the credit stuff's pretty well. I think the opportunity is in the operational risk space because I don't think we do enough, we generate enough insightful information about where we lose money from operational risks, and I don't—and it's hard to take that to particular products and particular processes. That's our gap. I don't know if it's the same for all organisations, but we collect good data that says this is where we lose money but it's really hard to aggregate at a product process–so you can go back and say the problem is with the design process, or the product is with this particular part of distribution.

Researcher: 52:41 Do you think that it's the process or the reporting?

Tier 1 Participant: 52:45 Well I think the reporting then allows you to identify the process so I think it's two steps. I think they're related.

Researcher: 52:57 I would like to thank you Tier 1 Participant for the valuable information. Thank you very much for that and really appreciate your support on this.

Tier 2 Sample Interview

Tier 2 Participant: (01:09) I received the document you've asked me to sign and I'll send that back to you after the call, if that's alright.

Researcher: (01:21) Yeah, thank you for that.

Tier 2 Participant: (01:22) That's okay. Alright, where do you want to take off from?

Researcher: (01:29) You asked me last time about which division I was working. Yes, I was working the risk division under the operations side.

Tier 2 Participant: (01:42) Yes. I think we've kind of gone through the flaws haven't we, last time. You sent me an updated–

Researcher: (01:52) Right. Basically, the current Reality Tree, the one that we have spoken about last week which represents the actually situation in the financial institutions. We have identified four main core effects that affect or increase the level of the risk that the financial institution is facing. I have categorised those elements which is in a control failure type
which is either people central or from the extended service provider, disruption, or regulatory, or the last one which is technology have failure. This is that core control failure type.

Tier 2 Participant: (02:40) Yes, what we were talking about. The only one that's missing there from my view would be process. There's the people failure, but an actual failure in the process itself, the way it's been set up.

Researcher: (03:00) Yes.

Tier 2 Participant: (03:01) When you're with that one stage.

Researcher: (03:03) Yes, I agree with that and that one represent in slide number 18, if you see, that has the process. The complicated tree.

Tier 2 Participant: (03:15) I'll have to go back to your slide. Sorry, I'm sort of jumping between that one other one. So slide 18—it was that?

Researcher: (03:23) Yes.

Tier 2 Participant: (03:27) Whereabouts? I can't that here, sorry. There's quite a bit going on the slide so I can't see.

Researcher: (03:34) Slide 18 and it shows the interaction between each element affecting the operation side from the front line to a business side. For example, if you go to the demand core effect or issue, if we have inadequate staff training (they haven't followed the process or they haven't followed the policy that the financial institution has), that will affect the operations side in terms of there can be a human error in database. That one can cause demand compliance risk. For example, what happened with BankA. One of the staff has entered a transfer 5 million to different client. That will cause damage for BankA, as an example. So we have to have a process in each equivalent place and each staff have to follow the procedure that we have in the financial institution.

Tier 2 Participant: (04:36) I guess to me, you see that it can be related, but it could be different. You could have a process that's perfect, but then the staff member misunderstands or doesn't follow up, so then it's a human error. But you could have a process that's actually imperfect and the staff member follows it perfectly, so it's not a human error. It's actually that the process is flawed.

Researcher: (05:05) Yep, I'll consider that. I'll put in my notes, yeah.

Tier 2 Participant: (05:07) I think it could be different. They're often related. They're often, you know, the process isn't fantastic, the person following the process makes a mistake, leads to, as you said, a compliance type of effect or it could relate to an execution delivery processing-type error that might or might not be compliance related. They're often together, but they can be different and I think I certainly have come across a number of risks or even ones that take place where it has been a process that's flawed and the person following it has followed it properly, but the actual process is still the incorrect (05:52) style.

Researcher: (05:52) You mean by process, the actual framework in the way that reporting from one division to another division, or engaging?

Tier 2 Participant: (06:00) Well, it could be any sort of process really, so it could be how we
transfer funds between banks over ten years old. There's a written process around that and that will have a number of controls built into it, but the person executing that process, following it, could follow the process as it's written and if there are errors in the actual way that it's documented, you could still end up with a risk or an actual effect.

Researcher: (06:40) I agree with that and I'll consider that and I'll try to allocate and adjust the framework that I'm developing to what you have said. This is what you see in slide number seventeen, which is the current situation in the financial institutions. Do you have any suggestion other than that process to consider?

Tier 2 Participant: (07:12) On that one, what I was saying was that I felt there were other types of risks as well, under risk category. I felt that that wasn't complete. If it were me, I would put regulatory risks and compliance risks under operations risks—that's just how we see it.

Researcher: (07:35) Okay.

Tier 2 Participant: (07:37) I think your conduct risks can sometimes be seen under operations risk, but it can be separate. Obviously, you've got credit risk, but I think that the context of the financial institution you've also got market risks and interest rates in the banking book. Strategic risks and reputational risks. I think there's probably some others that maybe could be called out as risk categories at that forward level.

Researcher: (08:10) Yep, reputation, culture, and market risk.

Tier 2 Participant: (08:15) Yeah, I don't know about culture. I think in culture risk and conduct risk—I would see culture as being part of a cause above a risk, personally.

Researcher: (08:34) That's okay. Thank you for that. I really appreciate this. I'll adjust in there with what you have added as well. Regarding the document that I have sent to you today, the future Reality Tree, have you had the chance to--?

Tier 2 Participant: (08:57) I haven't had a good chance to look at it, but I'm happy for you to walk me through it while we're talking on the phone.

Researcher: (09:03) Sure. That one is similar to a current Reality Tree. The current Reality Tree represents an actual situation and the future Reality Tree which represents how the bank needs to be run in the future. We said earlier, there are four effects or causes that cause financial supply chain risk, which is demand, supply, product management, and IT core effects. Then we go to the second layer. This is the main points that the bank needs to consider in terms of controlling the risk that they're facing. For example, people central failure. Another way that HR—each business unit has to report to the HR, however also they need to engage with a different platform to make sure that when they're recruiting any manager or staff, they have to have their own procedure. But if any risk that involves or happens should be registered in the risk register and that one aligns with the operation risk library. That can be from internal and external as well.

Tier 2 Participant: (10:23) Yeah, is this at a core level though and what you were saying—that the people will enter failure? That's a cause or an actual risk?

Researcher: (10:33) This is a cause.
Tier 2 Participant: (10:35) Yeah, okay, so it'd be a cause of a number of different risks. People failure could be a cause or, when you look at the other types of risks, things that you catch and it could be a compliance risk, it could be a fraud risk. It could be an execution risk, processing-type risk. People failure could cause, really, most of the risks that we've got, of the types of risks that we look at.

Researcher: (11:08) Yes, that's correct.

Tier 2 Participant: (11:10) Yes, okay.

Researcher: (11:14) That one aligns with ***** framework?

Tier 2 Participant: (11:17) Yep.

Researcher: (11:17) Also, I was looking at the ***** as well as the risk registry, what they have, and try to build the framework that I'm doing, try to align with APRA as well, with moving to the top on risk themes as well. Let me go back a little bit. If we read this document from the top to the bottom, represent the functional level of the organisation. If you read it from the bottom to the top, which is representing the risk. From the side which is the division, each one, from the corporate level to the business level and operation or frontline level. In the green after the control failure is the operation risk library and that represents the risk category one and risk category two.

Tier 2 Participant: (12:12) Yes, that's what I was just talking about, so internal fraud, external fraud, and client product processes, etc.

Researcher: (12:20) Sure. In case there's any risk or there's any incident, we have to look at how we are going to respond to that incidence. To take action, we need to design, respond, and operate and take an action. For example, if we have control failure, either by effective or ineffective, we have to put that recommendation and it should be mandatory. That one–each one–see in the small box there, design and operate an action that respond to that people central failure. The second one which is recommendation and mandatory and business assessment also responds to the extended service provider disruption. The third one which is above control and effective in terms of the way that they look into the change or process or action. Underneath that operation side, we have to monitor and report to the higher management level. However, if you look to the design and operate an action in the business strategy, compare to that design and operate action in operation or front line operation strategy. So they have to engage between each other to identify and to align what's happening in the operation side with the business strategy because they have to communicate between the business and the operation side because the operation side is executing what the business request. This is the engagement between each business unit from the operations side to the business side. If you go up, for the business strategy, we have also monitoring and reporting centre as well. That will be collaboration between business strategy with a corporate strategy with that CF and COO level. Also, we have that culture adaption as well for all the organisation if they adopt the risk appetite level in between each business unit or each division. What do you think? Any suggestion or anything that I need to consider from your perspective please?

Tier 2 Participant: (14:54) What's business risk library? What does that mean?

Researcher: (15:00) Business risk?
Tier 2 Participant: (15:02) Library. The top one, in your business strategy box on the right hand side. There's a thing called business risk library.

Researcher: (15:13) All the risk that's involved in the business side in addition making in strategy and level of the appetite as well.

Tier 2 Participant: (15:27) Look, I understand where you're coming from. It's a different way of presenting it, but I think in reality that is how things should be working. I don't think, to a large extent, that is how things are operate within our business. If I go bottom up, which is what you've done, start a business tree in that level, we would identify our risk based on--and we would look at the causes of those risks and, depending on the size of the risk, we would make a decision as to whether we're going to treat the risk and if we're going to treat the risk or do something about it, then we would move into what you've got here, which is around action, so we would say, "Alright, what treatment plan or action plans are we going to put in play?" Which is really, "What controls are we going to build?" and we would look and say, "Alright, well how should the control be designed and how should it operate effectively?" Effectually, when it becomes a control, we would document it and specifically note how it's designed and how operates and we would test almost to be compliant. It will--you're doing it to make an assessment and to me it's built up into whether you decide to do something about it raise it some or just sort of nicer to have actions where some will be mandatory. For example, if we know that there's a piece of legislation that's coming into (17:18) for some at the end of June. It's mandatory that we put in place a project or piece of work to make sure we're compliant with that and see how that works. I think if I understand what you're saying with the control centre that's around testing whether the controls are effective or ineffective or if it's based on out of another area. Is that what you mean by that?

Researcher: (17:45) Yes.

Tier 2 Participant: (17:46) Yeah, okay. And then we would go up and where you've got business strategy, we've rolled everything up so where you've got monitoring/reporting, we've rolled it up to a divisional level and at a divisional level, we would have--that's where they look across each of the businesses within a division, but they also would look at other divisions as well that are either part of their supply chain if you like, so if you're sitting in our retail area like our branch network, you'd want to be having a look at the risks that the products area are highlighting because obviously if you're in the branches, you're selling the products that is designed by the products area. You want to be seeing what the risks are end to end on by a mortgage product. That can roll up at that level and then there's a bit of layer reporting that I've found at the corporate level, at the brick level again, which is really looking across all of the divisions. Seeing how they all link in together and that's really looking at what I call key risks, the ones that are material and if they were to increase, the ones that we'd end up with a very large block or effect. That's kind of where you're sort of thinking about things. I wouldn't say that all of that works perfectly in reality at the moment, but it's certainly where ideally we would be going in a powerhouse framework you set up, so I think it makes sense. When you said risk themes, we do look at risk themes at a root level as well, so we'll take all that bottom-up information and we look and we say, "Alright, where are we seeing the concentration in these particular types of risks?" but we don't do any other--other than any what we've talked about--risks, but we look at it on a theme level and we'll say, "We're seeing--did it work?" in the space compliance or annual, so we would say that's a risk theme. We then have to indicate it around that theme that we monitor and report on. That's sort of top-level. I think what you've got here is probably (20:25) how. It's not exactly,
but obviously you're looking across a number of institutions, but I can see how what we do would be do too (20:32) deep for you for here.

Researcher: (20:35) Also, I have adopted agile practice in your theme of continuous improvement in each division and each business unit.

Tier 2 Participant: (20:44) Yeah, we don't do agile here yet. We're about to, but I'll sort of understand what you're getting at— that's an iterative approach that you file and see type theme where you have a look at something and you're continuously and dynamically updating your risks and monitoring all that kind of stuff. I agree with that then.

Researcher: (21:10) The thing that adopting agile to add value from the top level of the organisation. That is one of the key elements that scan monitors. What's happening in the business? How is that also, in the level of the business or business unit? I'm going to use Kaizen as well, contraction between agile and Kaizen in terms that each business unit uses which business practice suits that business unit.

Tier 2 Participant: (21:43) That fits in pretty nicely I think around your actions because quite often, by documenting your risks and your control, we can actually find that you may have too many controls as well. That's not always the case, but you find that you've got five controls where you could have one and therefore you've got a lot of processes that are redundant so you're not really doing them for any particular purpose and I can see how your lean principles fade into that process of improvement. The leaner your process is, the less likely where you're going to have process cause to as well.

Researcher: (22:29) Yep, I'll write it down, leaner process. That's what I'm looking for, just to verify what I'm doing. I'm on the right track. If I need any further update, I'll consider any change that you have, I mention, which is the process and also major compliance with the regulatory as well and also you've got in there reality tree have the control be and what the key risk or main risk and also the leaner process. I'll look to that as well. Then I'm going to update the framework that I have now and I'll keep you posted about what I am doing.

Tier 2 Participant: (23:16) Okay, alright. That sounds good. So do you need anything else from me at the moment?

Researcher: (23:21) No, thank you. I really appreciate that.

Tier 2 Participant: (23:21) No, my pleasure. I'll provide you with that sign-off for your record as well. I'll email it to you after the meeting.

Researcher: (23:35) Are you able to share with me some operation framework? I'm happy to sign a document that's a confidentiality agreement.

Tier 2 Participant: (23:46) I'd have to check on that to be honest. I'd have to double check about whether that's okay or not.

Researcher: (23:52) Yeah, that's okay.

* Tier 2 Participant: (23:57) I mean, I've looked personally, so it doesn't really bother me. I don't think there's actually a huge amount. I think you'll find that the bank frameworks are going to be largely aligned because of the interaction with that firm. I think they're all going
to be pretty similar and they've been largely aligned to what you've got here, to be honest, because what they do is look at the first to each of the banks and they may recommend that the other banks start following that so you'll see a convergence in what all of the banks are doing. We get together with the banks quite regularly as well, so I don't know. You might be already aware of this, but there's an inter-bank operational risk forum that all of the banks—the heads of group up risk from all the banks become, and then there's another group as well which is just the **** or the (24:58) ******. There's a lot of sharing of information so everyone finds ways to keep in line.

Researcher: (25:07) That's good.

Tier 2 Participant: (25:07) You can ask a question about it. I'm just not really sure whether we normally would disclose that, so just leave that with me.

Researcher: (25:15) Well, yes, some of the banks they share with me.

Tier 2 Participant: (25:19) Yeah, ours will be very similar. There's not a lot of (25:22) goals for very difference that I've seen because we're so dictated and regulated by (25:31) APRA and so you pretty much end up all being quite similar, I think, in the way that you operate.

Researcher: (25:37) Yep.

Tier 2 Participant: (25:38) The other reason is a lot of similarities between the banks—I think I mentioned this to you last time—is the because of subscriptions to ORE. They are very descriptive on the way in which in you need to categorise—effects that have happened and I guess the consistency you bring that across into your risk categorisation as well, so you see convergence around your causes and risk libraries and stuff like that as well.

Researcher: (26:10) Yeah, I was in touch with APRA and they gave me some information as well. Yeah, I tried to cover up all the different platforms from tier one, tier two, tier three, which is I find there's big gap between tier one and tier three in terms of the way that managing the risk.

Tier 2 Participant: (26:35) Yeah, tricky. I mean I (26:37) pretty generally leave here too, but we just got advanced accreditation from an operative perspective, I mean in February. We sort of probably (26:55) some operating systems, more up around tier one. In town, I think we're doing stuff, I think now.

Researcher: (27:02) That's good. The last question—I don't know if I can ask or not. Is there any opportunity after I complete my study?

Tier 2 Participant: (27:18) Within the bank?

Researcher: (27:19) In the risk division.

Researcher: (28:39) Thank you.

Tier 2 Participant: (28:40) No, my pleasure. I'll come back to you about the framework, whether we can disclose that, and I'll send that document off to you as well.

Researcher: (28:47) Yep, thank you very much. I really appreciate your support.
Tier 3 Sample Interview

Researcher: (00:00) Good afternoon Tier 3 Participant. Today we are going to ask you a few questions about our research and the topic is financial supply chain risk. One of the supervisors is from RMIT University and the second supervisor is from Monash University. The topic is about to validate the cause of financial supply chain risk and to see the relationship between the financial supply chain risk and the performance of an institution. We have selected senior risk managers from different financial institution. We are going to go over tier one, tier two, tier three. The first question, Tier 3 Participant, could you please tell us about the background and the experience that you have done so far in the financial and the credit and the risk that's involved in the banking industry? Those three I know that you have extensive experience that have been here years and years.

Tier 3 Participant: (00:55) So just in financial services?

Researcher: (00:57) Yep.

Tier 3 Participant: (00:58) I guess I was at BANK for six years from 2000 to 2005, in two distinct areas. One in the credit card business, was head of fraud and compliance and then head of operations for the cards business, so pretty hands-on role looking after unsecured lending environment for BANK in Australia. Then moved to a global op risk program for BANK looking at developing advisor to op risk program. I kind of led that for a couple of years. Next bit of financial services, specific experience would be when I joined ***** in 2007. I was there for about five years or four and a half years. More than half of my clients were in financial services so it was a lot of work in reviewing building risk frameworks, doing risk strategy, risk appetites, some supply chain specific stuff, but brought up a broad range of risk related activity. The next most compelling financial services would probably be coming to M***** about a year ago and working here. I’ve worked in, as you pointed out, a number of different industries. Risk is very transferable, but the content has been specifically around field services in those places.

Researcher: (02:41) Okay. Second question: what are the significant changes in the tech that you have seen in the financial risk division in the last two decades?

Tier 3 Participant: (02:53) the principal one, probably, is the ability of technological innovation to better manage or share, communicate data risk related data so that it’s much easier to make more informed disbursed decisions of these days because of the tools and data that's available.

Researcher: (03:14) So you’re you moving from a traditional system to a digital system.

Tier 3 Participant: (03:19) Yeah

Researcher: (03:19) It does look exactly how I put in here. What’s about the models? What is a change that you have done or you have seen in the last ten years in that financial industry models?
Tier 3 Participant: (03:32) I think the models are changing because the risk needs to be, in many cases, close to real time, depending on which part of the business you're talking about.

Researcher: (03:45) Yeah business banking.

Tier 3 Participant: (03:46) But in supply chain, for example, you either want real time or near to real time risk data or risk decisions and therefore what’s changed is how embedded the risk process is in the supply chain process.

Researcher: (04:02) Exactly. I was reading what's called RMJ–Risk Management Journal. I have been reading all the things what’s happening in the last–I'm a member with them as well so I try keep myself up-to-date what's happening in market as well, not only just in the academic side as well as the banking industry side as well. They have some good article on what they accomplished, so operation risk, enterprise risk, and all those things. Category, what they have categorised into each different section, that which is diagram. Third question: how would you maintain the necessary knowledge and skills? For example, what's the strategy that you use for the staff here to update or to keep them motivated about what's happening in the market?

[Interruption 04:48-04:57]

Researcher: (04:57) Question for you: how would you maintain necessary knowledge and leadership in the risk division?

Tier 3 Participant: (05:03) Two things–in the way our team works, we have a mandatory education among.

[Interruption 05:09-05:20]

Tier 3 Participant: (05:23) I'm a big believer in education and lifelong learning so in my team, I mandate one hour of mandatory industry reading for the team every week, but we also have a big focus on different tools that make sure people are educated, informed. We use tools like Yammer, which is an internal social media tool to post interesting documents and updates, share all our information and probably operate under the philosophy you share everything except remuneration information so there's a lot of in-sharing. Everyone has their own individual development plans where you formally put people on the programs for the year, whether they want to do post-grad or whether they're doing some kind of self-paced study. There's a lot of a lot of free stuff as well so it won't necessarily be expensive.

Researcher: (06:22) Exactly you're saying about, I was expecting that because anybody or a newer department about what about that FRM, if anybody has a certificate or something like that, production of development or commercial education side, I would call it like.

Tier 3 Participant: (06:37) A lot of the people I recruiting because the team is 60% recruited by me in the last eight months so I recruit for the right balance between educational experience and probably people skills or networking.

Researcher: (06:54) Networking.

Tier 3 Participant: (06:56) A lot of those people have got high level education levels and we don’t have a mandatory requirement for any particular qualification and I’m not necessarily a
big believer that you should go and do a particular course because you get a FRM or something. I’d rather have–because the world is changing so quickly that some of those courses actually aren't that relevance so it's a mix of different skills that sometimes are outside the formal education process.

Researcher: (07:29) That's good. What determinants the effective Financial Supply Chain Risk?

Tier 3 Participant: (07:33) Say again?

Researcher: (07:36) What are the determinants that are affecting the Financial Supply Chain Risk? For example, demand operation or new system operation or supply operation or product management or any other you happen–

Tier 3 Participant: (07:46) A whole lot of things, but I think that one of the biggest–there's a couple of factors. One of them is them is commercial understanding. One of the biggest challenges is that we have, sometimes, is we have a whole host of third-party relationships which power the supply chain, which we have because we need to have them as a retail bank, but they haven’t been created in the most commercially sensible ways because it's a lack of contractual knowledge by either party or it's a lack of understanding the broader domain in which those contracts or relationships are formed.

Researcher: (08:27) –asking me about the contract and about other things.

Tier 3 Participant: (08:31) Yeah, I've also got a background too so I focus heavy on contract rights and obligations in real-life third party relationships.

Researcher: (08:37) Yep, Dicken university, graduated from law.

Tier 3 Participant: (08:40) Yeah, you did do your research.

Researcher: (08:42) Oh yeah.

Tier 3 Participant: (08:43) But practically, a lot of costs that are embedded in supply chain are because we don't set them up well and then secondly we don't manage them well, so there's two key parts to it: contract formation and contract management.

Researcher: (09:01) Or contract knowledge

Tier 3 Participant: (09:04) Yes so the contract formation follows having superior negotiation skills based on knowledge, education, understanding of the domain. Everything from a why did we lock in a three year contract when we know that technology is changing, we should only go for a 12 month contract. The cost of production is x but we can see there's innovation overseas–it should be y.

Researcher: (09:27) Especially in IT industry as well.

Tier 3 Participant: (09:29) Yeah, so we just lay the whole piece of work reviewing our IT security capability across the bank which has led to a whole three year program with work that the board has just approved, which fills in gaps in our supply chains which relates to IT security.
because we took a fresh look at what’s the state of the world more broadly and how rapidly are things changing.

Researcher: (09:55) The technology, especially in technology. Now look to the bank in more being–I was looking at BANK's strategy. In order to digitalise and also the other example if you remember. When BANK and ***** used to have same return until ***** between 2000-2006 they have changed their IT systems

Tier 3 Participant: (10:18) Yeah. ***** drove a massive program and different to BANK, so my perspective theory is projects can get too big unless they’ve got absolute discipline to the top–cut through clear strategy, clear objectives, and that's not the case usually.

Researcher: (10:41) That is exactly–

Tier 3 Participant: (10:42) So next June from BANK–

Researcher: (10:43) This June they have been working with it for three, four, five years and I was talking with one of the executives in ***** and he said to me, "No, no. (10:52) What's that?" I said, "I know about next June what's happening up there." I don't know if the project's still working or they're going to centralise everything and the course involved, but they're spending a lot of money, but it’s too late I think.

Tier 3 Participant: (11:06) Yeah now that they've wasted so much money.

Researcher: (11:08) Yeah, I don’t to say that at the moment.

Tier 3 Participant: (11:11) I'll say it. They've wasted so much money.

Researcher: (11:14) And the person who was implementing this program in the first place, David Thompson. And he left. Now they still have the last few years doing that. But you know this last two minutes that you answered this questions and the other question about the contact, about supply contract, or the order allocation and supply relationships, and all those things. Other question what does information system management impact? How would information system manager impact the organisation?

Tier 3 Participant: (11:46) I ran around supply chain.

Researcher: (11:47) Around the risk.

Tier 3 Participant: (11:48) Ran the risk around supply chain. Clearly there are a whole bunch of systems that help you manage your supply chain risk. In Michael's world, contract management is a very sophisticated domain if done properly because you need to manage to your SLOs, you need to manage the emerging risks, not necessarily reflected in the contracts, so it’s not just managing what you have signed up for. It's managing how the risk is changing over time.

Researcher: (12:20) You have to be up to date what's happening in the market. What about outsourcing? What's in play?

bbb: (12:27) Well clearly there's an APRA standard that is relevant in terms of outsourcing and recognising the account–outsource your risk or your responsibilities necessarily, but we
tend—not we need as in me but we in the industry—tend to outsource without understanding enough about who owns the risk and what other what other overheads do you need to actually manage the process well, but again, technology is the 50% eBankler and support for managing risk in supply chain because it it’s the mechanism by which you manage your data and do the analysis to make better decisions. It's the transmissive conduit for the sharing information and presenting information.

Researcher: (13:23) Which is exactly my philosophy. I think maybe you agree with me. When I'd done my study I said, "I want to do in bachelor in IT," and then I done bachelor in IT and then after that I said, "I work in IT. I want to do a masters in finance," and then I did a masters in finance and then I said, "I want to do in accounting" and then masters in accounting. Then my family and (13:47) my sister said you are busy, why this study? For example when you drive your car and you have alarm and you ignore the alarm and after that what will happen to your car? You will stop in the middle of the road and you can't do nothing, so exactly this is the risk. Risk is good indicators for us to see what's happening in the business and what's going on in the business but unfortunately people have different perspective.

Tier 3 Participant: (15:03) Risk is more important than ever, I think, in supply chain because other issues like first mover advantage and if you're looking to be really commercial you want to get into emerging spaces before anyone else or lock in better pricing or better arrangements so to do that you need to—to me risk is just about making better business decisions

Researcher: (15:28) Okay. I agree 100% with you because you exactly monitor the business what's going on, but what the about now complexity and simplicity in the IT system.

Tier 3 Participant: (15:39) I guess my view there is you have to look at materiality and have to have proxies for managing complexities. You have to have the right tools to turn—you can't talk chaos theory and massively complex scenarios every day of the week if you're talking to the exec about making a business decision between options so you have to have a mechanism to—

Researcher: (15:59) –support your decisions.

Tier 3 Participant: (16:01) big data down to, here's an AB decision. How do you do that? It’s not just technologies. It's also intellectual curiosity about the best way to take what matters into a decision so in some ways it's stripping out a lot of noise.

Researcher: (16:19) That's good. What about the impact of the product management, like a new product, life cycle, innovation, in-house built, or outsourcing, or any other you have?

Tier 3 Participant: (16:32) We are developing products in ME and we’re not doing it necessarily in the best way that we can all the time because you’ve got to have all the right minds around the table when you making product decisions because a lot of the things that will hurt a product's success are not the things that the product manager thinks of at the very first instance. They will be things like the ability of the supply chain to actually meet the requirements of the products. So that's a live example of something going on at the moment. So you think, Well base a product on XYZ, but and if the vendor can’t meet those timeframes, the cost of leaving them is carving to the benefit. There is innovation disruption happening in that space. Did you not see that? There are compliance complexities to that which we are not mature enough to manage so you've created a product which is beyond our compliance
capabilities. I think the answer is you're going to have all of the SMEs, or subject matter experts, contribute.

Researcher: (17:45) Knowledge or experience expert, you mean?

Tier 3 Participant: (17:47) Yeah, it's both, I suppose.

Researcher: (17:53) Okay. Can you just give me a small, brief explanation between the financial supply chain risks? When I'm talking about the Financial Supply Chain Risk, about the money movement, about cash delivery, about a product that they have—a mortgage and all that thing—and the performance of the financial institution. What’s the relationship? Or there’s any what the factor for KBI, because another example, like BANK now they're giving 40% of their scorecard on the risk—40%. And the XY Bank, they’re given 35, something like that.

Tier 3 Participant: (18:29) Yeah, so executives?

Researcher: (18:30) Yeah. I'm talking about that because it's not about operational. What about a new bank and what you think about that? What’s the relationship between Financial Supply Chain Risk and the performance and what’s the KBR indication that you have?

Tier 3 Participant: (18:45) We have a minimum of 10% KBR for executives on risk generally, so risk identification, risk management, so regardless if it's supply chain or something else, which is too low but that's just a starting point. So 30 or 40% would be great because basically every decision they make is a risk-based decision. It's more a cultural change. I just got to look at the loss effects that any organisation has incurred or the lack of business case benefit realisation when you look at the new product or something else which hasn't been captured by a loss effect, so you're looking at: what do we lose and what did we not get the benefit of and look at the root causes of that. You can look to the supply chain and go, "Well, we didn’t know enough, we made too many assumptions, we didn't have the required maturity in the system, we didn't engage more broadly across the business, we didn't have the right contracts or rights of obligations." So there are so many ways to have negative performance in the business by not managing all those critical success factors in the supply chain.

Researcher: (20:04) Okay. Do you think about any other (20:05) re practitioner you are using in your organisation, in addition? For example, six sigma or Kaizen? What do you think about Kaizen and continuous improvement theory?

Tier 3 Participant: (20:15) Well I think it’s good in particular environments. For supply chain, I think some parts of the supply chain it does make—pretend, for example, if you are developing a new car product and looking to a new car manufacturing process and you want to look at ages/HR's head of that whole process, but I think a lot of executive thinking is so removed from the disciplines of the Six Sigma that there's too much biased emotional stakeholder judgment at that level

Researcher: (20:58) Especially about the number of the debt that we have collected. Everyone gives you their own.

Tier 3 Participant: (21:02) Yeah, absolutely. It’s not enough discipline on the way through.

Researcher: (21:06) What’s the relationship—do you think that Six Sigma or Kaizen affects the relationship between the Financial Supply Chain Risk and the performance of an organisation
if we ever implemented in our organisation. For example, we have one of the big auditing company uses Kaizen and they have reduced the costs to 40%.

Tier 3 Participant: (21:28) Yeah, the answer is absolutely yes. I just think you need to tailor it for different parts of the supply chain; one size doesn’t fit all.

Researcher: (21:40) Definitely, there's the exception.

Tier 3 Participant: (21:41) Yeah, so if you look at your legal services providers, for example. I wouldn't use Six Sigma on that.

Researcher: (21:45) Exactly. No, you can't. It's a different industrial so you can't use everything or make the--for one thing in one industry, you can't use in all different structures.

Tier 3 Participant: (21:59) But I would use it, for example, if you’re looking at the homeland chance or broker channels for examples. You could do end-to-end of the broker origination. You could do something there. Credit cards. All the standard retail products but not a sophisticated bank so all those things could be done. It's more you're eBankling services like your insurers, your legal services, advertising--you could probably do that too.

Researcher: (22:21) Okay Tier 3 Participant, thank you very much for that information and that the great information that you have provided and I really appreciate that you support

Tier 3 Participant: (22:29) No problem.

[Static]

Collated participant quotes from informal validation interviews (various dates)

Tier One Participants

Participant 1

- The different banks are often very similar, in my experience of the sector, despite volume differences in retail or wholesale banking, or the range or mixture of other financial products offered.

- Certain issues which I can put down to lack IT knowledge, which I can put as a supply chain system failure, which I can put in human errors and all that. I know the impacts to the business in terms of tests happen that we are approving loans by--there's a service agreement complement, like where the person can service that loan amount so an error is causing the customer's income to be calculated incorrectly which means you'll get a loan, even if you are not earning that much. So that's a major impact and that's happening in some loans. Capacity and capability are what comes to mind. Where you've got here--staff capability--it's part of that and I do see it coming from supply issues. We're also talking about resources. Across our point of view, I see those are the main drivers for HR issues. From a capability and a capacity. You manage those two things in HR, usually that translates to a bit of a cross, which is what you've got here.
The effective implementation of corporate risk appetite driven control over product risk is often blocked or reduced by a silo mentality of individual areas. They go about their business somewhat disconnected from controls whose intention is to monitor and moderate risks, but these intentions often don’t bear fruit because of the disconnects, and can cause issues I’ve seen with swapping exchange rates for example.

We want the big plan about how to apply all the risk reduction and control processes. What happens now where we might have similar things in place, is that each of these systems or processes at times start looking silos. So then developing silos, they become kind of quite obstinate about what needs to be done, how it needs to be done. There should be a flexibility. There should be plans and guidance’s.

**Participant 2**

- The common denominator across credit risk, operational risk, all these types of risk, is the risk management framework that sits in its own bubble and that drives issue management, change management, obligation adherence, compliance adherence, operational risk business environment, definition, and how I said what the most important thing is would be risk appetite settings at the very top. That framework should ideally drive all this interaction and provide input into process improvement after the fact.

- The challenges that banks historically have had large, big, monolithic, centrally run technology systems which are incredibly hard to maintain, incredibly hard to update large amounts of investment that require multiple years of delivery to do. That's not the customer's experience when they can get a new app in three seconds right now and if they don't like that app they'll go and try another one. So that's part of the challenge we're facing is that we have a business model that's based around having central, everyone access to the data and customers are used to providing their data to 25 different apps, but that each of those apps are something very unique, very specific, and very value adding for the customer, and that's the challenge we're facing.

- Technology, absolutely. We are increasingly reliant on outsourced or third-party providers. I'm interested in HR and the payments process. This is a consequence of that. We're saying is there's also driver there that relates to the impact that regulations and policies have on how the business can do—what activities they can do and how it can do them. On top of that, if the staff aren't trained well, then there will be errors leading to compliance risks and other impacts. Not enough people, capacity, capability—all those sorts of things related to people skills So it is a cultural issue and an HR issue. In operational risk, we talk about people, processes, and systems. You're aligned.

- In our organisation, the responsibility for training exists with the business, not the HR area. So those failures or the drivers that relate to people. Its people-centred failures, that would include error, lack in training, lack of capability. This is a pandemic that fuels multiple risks—all of those sort of things—not enough people, capacity, capability—all those sorts of things related to people skills

- Capacity and capability are what comes to mind. Where you've got here—branch staff capability—it's part of that and I do see it coming from supply issues. We're also
talking about capacity? Across our point of view. I see those are the main drivers for HR issues. From a capability and a capacity. You need to manage those two things in HR.

- Whether its big IT, retail issues affecting customer satisfaction, risks with product development outsourcing, or just that are so big and diverse, we have written off large amounts because the risk trade-offs are wrong. Because we didn’t understand properly. We need a system of controls that can get good intelligence about risks to make better decisions and to more effectively implement controls, I think the what you show here, reflects well how things should be in place.
- It's important that communication and messaging comes from the top. Communications and messages, some of the policies and messages that get rolled out has to come from the top and then that disseminates across the organisation’.

**Participant 3**

- It looks like risk is like snow balling picking up momentum and increasing in size as it rolls along.
- that would include error, lack in training, lack of capability. You know, pandemic–all of those sort of things– we need enough people, and to build their capacity and capability– all those sorts of things related to people skills that causes issues across the board.
- Effective collaboration and monitoring are critical elements in the central role of the interface between the corporate side of the business and can have real impacts on operational risks. Risk mitigation action that is well coordinated, mutually informing and communicated can have a positive effect on things like training, recruitment, customer service levels and innovation. You really need a strongly connected and aligned supporting context that is cross-functional...

**Tier Two Participants**

**Participant 4**

- And then cross divisional collaboration. It’s very difficult. I don't think any company has got that down pat. It's too difficult. …To get uniformity, whether it's in processes, whether it's in procedures, whether it's in reporting, is very difficult and takes a deliberate and planned effort.
- “the push to outsource has produced efficiency benefits but perhaps at a cost of increased risk that was not foreseen through reduced internal capability to control the risk”.

**Participant 5**

- One of the problems that you've got in major financial institutions is people in divisions like IT don't see a full vantage of it. That's the operating effect that's occurring within the value chain, if you like, because one of the problems that you've got, for example, usually ATM failure. You may have been able to avert that if you had sufficient capacity to apply controls over that to actually identify the problem earlier or even
before it occurred. The actually underpinning of cause of not having a control, but the
reason why it didn't have a control over it was I didn't have enough capacity in my HR
to build a control.

- reference to culture, I have a saying that you can create the perfect mousetrap. It’s not
an original saying, but if people won't use it, it's useless. So, I think your risk design,
you're getting the full value chain, working together, owning responsibility. That comes
down to your culture, so you've got to make sure that culturally that is seen as the
preferred direction. You've got to make sure you don't build the pocket of resistance to
the culture of the organisation.

- “It has an impact on their reputation, bank reputation, and safety because the bank looks
into the safety as well. The interesting factors that are starting to apply to my mind is
with digital technology, the customer can probably, in most cases, see what your
internal system can see. These layers of non-disclosed control, are starting to become
more and more blurred as the system starts to digitise themselves. What occurred in
that situation was they sought to maximise their capital market value in the short term
(instead of investment in IT risk controls) which is an unsustainable business model
and because they were doing it via cost control, not carrying business efficiency with
it as well, you effectually had a breakdown in controls and you had a calamity or
multiple calamities.”

- We have a whole host of third-party relationships which power the supply chain, but
they haven’t been created in the most commercially sensible ways because it's a lack
of contractual knowledge by either party or it's a lack of understanding the broader
domain in which those contracts or relationships are formed So the contract formation
follows having superior negotiation skills (person-centred) based on knowledge,
education, understanding of the domain. Everything from a why did we lock in a three-
year contract when we know that technology is changing, we should only go for a 12-
month contract. The cost of production is x but we can see there's innovation overseas–
gaps in our supply chains which relates to IT security. We need a fresh look at what’s
the state of the world more broadly and how rapidly are things changing

- What we had previously defined as independent risks and effects, they now appear
interconnected and they influence each other This is a highly complex environment that
we are operating in at the moment and we have interdependencies that, when you start
to think about them, you realise how interconnected everything you're doing is.

- The need for a consolidated view where for each performance unit, it does have an
effective control environment in place to mitigate the risks. You need to have a
reporting and collaboration centre between the business and the corporate level of the
organisation.

- ‘to avert risk effects in retail you need to have the control capacity in place to identify
and respond before it occurs to prevent it.’

Participant 6
- It could be any sort of process really, so it could be how we transfer funds between
banks over ten years old. There's a written process around that and that will have a
number of controls built into it, but the person executing that process, following it,
could follow the process as it's written and if there are errors in the actual way that it's documented, you could still end up with a risk or an actual disruptive effect.

**Tier Three Participants**

**Participant 7**
- it might vary in the very specific details and in the names given to a function in a particular organisation, but overall it is a reasonable representation of the generalised structure of Australian Banks
- If you're getting the full value chain, working together, owning responsibility. That comes down to your cultural adaption, so you've got to make sure that culturally that is seen as the preferred direction

- More leadership around reinforcing a view of IT external service providers, internal business needs and IT system integration should be more driven by delivering information that supports business decision-making rather than an unbalanced focus on isolated technical risks. You know, having a connected risk control soft-infrastructure in place is necessary to mitigate risk in the hard enterprise infrastructure.

**Participant 8**
- Through this process I have become more aware that for each of the core reasons, they were manifested by several specific unwanted risks that were related to each other, when they are not always seen that way in practice.

- The way I see it, the common denominator across credit risk, operational risk, all these types of risk, is the risk management framework that sits in its own bubble and that drives issue management, change management, obligation adherence, compliance adherence, operational risk business environment, definition, and how I said what the most important thing is would be risk appetite settings at the very top. That appetite framework drives all this interaction and provides input into process improvement after the fact.

**Participant 9**
- A lot of the things that will hurt a product's success are not the things that the product manager thinks of at the very first instance. They will be things like the ability of the supply chain to actually meet the requirements of the products. So that's a live example of something going on at the moment. So, you think, we'll base a product on XYZ, but if the vendor can't meet those timeframes, the cost of leaving them is carving into the benefit. There is innovation disruption happening in that space. There are compliance complexities to that which we are not mature enough to manage so you've created a product which is beyond our compliance capabilities.
- ‘in foreign currency options, part of the reason for the failures was that the managing office was under resources which in turn was because of human error and HR capacity and capability’.
- We in the industry--tend to outsource without understanding enough about who owns the risk and what other what other overheads do you need to actually manage the process well, but again, technology is the 50% enabler and support for managing risk
in the supply chain because it’s the mechanism by which you manage your data and do the analysis to make better decisions. It's the transmissive conduit for the sharing information and presenting information
### Risk Effect Type Level

<table>
<thead>
<tr>
<th>Risk Effect Type Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execution, Delivery and Process Management</td>
</tr>
<tr>
<td>Clients, Products and Business Practices</td>
</tr>
<tr>
<td>Internal Fraud</td>
</tr>
<tr>
<td>Employment Practices and Workplace Safety</td>
</tr>
<tr>
<td>Business Disruption and System Failures</td>
</tr>
<tr>
<td>Execution, Delivery and Process Management</td>
</tr>
<tr>
<td>Clients, Products and Business Practices</td>
</tr>
<tr>
<td>Internal Fraud</td>
</tr>
<tr>
<td>Damage to Physical Assets</td>
</tr>
</tbody>
</table>

### Risk Category

<table>
<thead>
<tr>
<th>Risk Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting Error</td>
</tr>
<tr>
<td>Bribery</td>
</tr>
<tr>
<td>Casualties from External Effects</td>
</tr>
<tr>
<td>Collateral Management Failure</td>
</tr>
<tr>
<td>Conflict of Interest</td>
</tr>
<tr>
<td>Damage to Physical Assets</td>
</tr>
<tr>
<td>Data Error - Incorrect Recording of Risk Exposures</td>
</tr>
<tr>
<td>Data Error - Loading</td>
</tr>
<tr>
<td>Data Error - Maintenance</td>
</tr>
<tr>
<td>Data Error - Manual Entry</td>
</tr>
<tr>
<td>Denial of Access to Facilities</td>
</tr>
<tr>
<td>Disruption of Technology due to Complex or Ageing</td>
</tr>
<tr>
<td>Systems</td>
</tr>
<tr>
<td>Disruption of Technology or Telecommunications</td>
</tr>
<tr>
<td>Employee Relations Failure</td>
</tr>
<tr>
<td>Employee Theft from Customer Accounts</td>
</tr>
<tr>
<td>Employee Theft from Group Company Accounts</td>
</tr>
<tr>
<td>Employee Theft of Information</td>
</tr>
<tr>
<td>Exceeding Client Exposure Limits</td>
</tr>
<tr>
<td>External Fraud</td>
</tr>
<tr>
<td>External Malicious Destruction of Assets</td>
</tr>
<tr>
<td>External Malicious Technology Service Disruption</td>
</tr>
<tr>
<td>External Theft from Customer Accounts</td>
</tr>
<tr>
<td>External Theft from Group Company Accounts</td>
</tr>
<tr>
<td>External Theft of Information</td>
</tr>
<tr>
<td>External Vendor or Service Provider Breach of Contract</td>
</tr>
<tr>
<td>Failed or Inaccurate Reporting</td>
</tr>
<tr>
<td>Health &amp; Safety of Employees or Third Parties Failure</td>
</tr>
<tr>
<td>Inadequate Advisory Activities</td>
</tr>
<tr>
<td>Categorised raw list of risks (interview derived)</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td><strong>Accounting Error</strong></td>
</tr>
<tr>
<td>Inadequate Model Validation</td>
</tr>
<tr>
<td>Incorrect Client Position/Transaction Status Reporting</td>
</tr>
<tr>
<td>Accounting error/calculations</td>
</tr>
<tr>
<td>Rates validation errors</td>
</tr>
<tr>
<td>Inaccurate/Incomplete Provision Assessment</td>
</tr>
<tr>
<td><strong>Bribery</strong></td>
</tr>
<tr>
<td>Staff Inducement Influencing Vendor Selection</td>
</tr>
<tr>
<td>Bribery</td>
</tr>
<tr>
<td><strong>Casualties from External Effects</strong></td>
</tr>
<tr>
<td>Causalities from External Effects</td>
</tr>
<tr>
<td><strong>Collateral Management Failure</strong></td>
</tr>
<tr>
<td>Inability to achieve securitisation targets agreed</td>
</tr>
<tr>
<td><strong>Conflict of Interest</strong></td>
</tr>
<tr>
<td>Conflict of Interest</td>
</tr>
<tr>
<td>Client confidentiality/conflict of interest</td>
</tr>
<tr>
<td>Failure to manage conflicts of interest</td>
</tr>
<tr>
<td><strong>Failure to manage conflicts of interest</strong></td>
</tr>
<tr>
<td><strong>Damage to Physical Assets</strong></td>
</tr>
<tr>
<td>Failure to Manage and Maintain Infrastructure Supporting Critical Sites</td>
</tr>
<tr>
<td>Loss of Commercial Building</td>
</tr>
<tr>
<td>Loss of PC and IT Equipment</td>
</tr>
<tr>
<td>Damage to Physical Assets</td>
</tr>
<tr>
<td><strong>Data Error - Incorrect Recording of Risk Exposures</strong></td>
</tr>
<tr>
<td>Counterparty Collateral Risk</td>
</tr>
<tr>
<td>Maintenance of customer information</td>
</tr>
<tr>
<td>Risk of failure to meet customer workplace and accommodation demand requirements</td>
</tr>
<tr>
<td><strong>Data Error - Loading</strong></td>
</tr>
<tr>
<td>Data Error - Loading</td>
</tr>
<tr>
<td>Payroll Management</td>
</tr>
<tr>
<td><strong>Data Error - Maintenance</strong></td>
</tr>
<tr>
<td>Master and reference data errors</td>
</tr>
<tr>
<td>Data Error - Maintenance</td>
</tr>
<tr>
<td>Failure to maintain policy changes and updates</td>
</tr>
<tr>
<td>Inability to ensure data integrity</td>
</tr>
<tr>
<td><strong>Data Error - Manual Entry</strong></td>
</tr>
<tr>
<td>Data Error - Manual Entry</td>
</tr>
<tr>
<td>Ineffective vendor payment processes</td>
</tr>
<tr>
<td><strong>Data Input Error</strong></td>
</tr>
<tr>
<td>Instructions/Payments/Confirmations missed or processed incorrectly</td>
</tr>
<tr>
<td>Instructions/Payments missed or processed incorrectly</td>
</tr>
<tr>
<td>Accounts Payable Error</td>
</tr>
<tr>
<td>Failure to ensure security interest held</td>
</tr>
<tr>
<td>Manual Data Entry Error</td>
</tr>
<tr>
<td>Transaction Establishment</td>
</tr>
<tr>
<td><strong>Denial of Access to Facilities</strong></td>
</tr>
<tr>
<td>Denial of Access to Facilities</td>
</tr>
<tr>
<td>Business Continuity</td>
</tr>
<tr>
<td>Denial of building access</td>
</tr>
<tr>
<td>Failure of Operations</td>
</tr>
<tr>
<td>Business Continuity - Business Interruption</td>
</tr>
<tr>
<td><strong>Disruption of Technology due to Complex or Ageing Systems</strong></td>
</tr>
<tr>
<td>Technology Failure Risk</td>
</tr>
<tr>
<td>Delays in service restoration of our complex, orchestrated technology environments negatively impacting business operations and customers</td>
</tr>
<tr>
<td>Data Quality/ Integrity</td>
</tr>
<tr>
<td><strong>Disruption of Technology or Telecommunications</strong></td>
</tr>
<tr>
<td>Disruption of Technology or Telecommunications</td>
</tr>
<tr>
<td>loss of technology support</td>
</tr>
<tr>
<td><strong>Employee Relations Failure</strong></td>
</tr>
<tr>
<td>Succession Plans</td>
</tr>
<tr>
<td>Staff Morale</td>
</tr>
<tr>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Loss of key personnel</td>
</tr>
<tr>
<td><strong>Employee Theft from Customer Accounts</strong></td>
</tr>
<tr>
<td>Employee theft from accounts</td>
</tr>
<tr>
<td>Internal Fraud</td>
</tr>
<tr>
<td>Internal Payment Fraud</td>
</tr>
<tr>
<td>Fraudulent payment instructions</td>
</tr>
<tr>
<td>Internal Fraud from External Instruction or Internal Generated Instruction</td>
</tr>
<tr>
<td>Misappropriation of fees/funds</td>
</tr>
<tr>
<td><strong>Employee Theft from Group Company Accounts</strong></td>
</tr>
<tr>
<td>Internal Fraud</td>
</tr>
<tr>
<td>Risk of Internal and External Fraud</td>
</tr>
<tr>
<td>Employee Theft from Group Company Accounts</td>
</tr>
<tr>
<td><strong>Employee Theft of Information</strong></td>
</tr>
<tr>
<td>Employee Theft of Information</td>
</tr>
<tr>
<td>Privacy breaches from inappropriate access to data</td>
</tr>
<tr>
<td>Internal theft of information</td>
</tr>
<tr>
<td><strong>Exceeding Client Exposure Limits</strong></td>
</tr>
<tr>
<td>Breach of credit limits</td>
</tr>
<tr>
<td>Verification Failure (Pre-Unconditional)</td>
</tr>
<tr>
<td>Unreliable and/or Inappropriate Valuations</td>
</tr>
<tr>
<td>Unauthorised Payments</td>
</tr>
<tr>
<td>Failure to undertake verification checks in support of the credit decision</td>
</tr>
<tr>
<td>Poor manual credit decisions</td>
</tr>
<tr>
<td>Middle Office Risk</td>
</tr>
<tr>
<td>Lending outside of Risk Appetite</td>
</tr>
<tr>
<td>Data Service Automatic price upload</td>
</tr>
<tr>
<td>Credit Assessment Failure</td>
</tr>
<tr>
<td><strong>External Fraud</strong></td>
</tr>
<tr>
<td>Fraudulent Lending Applications</td>
</tr>
<tr>
<td>External Fraud (microfinance applications)</td>
</tr>
<tr>
<td>External Fraud-loans used for unauthorised purpose</td>
</tr>
<tr>
<td><strong>External Malicious Destruction of Assets</strong></td>
</tr>
<tr>
<td>Service disruption due to external attacks</td>
</tr>
<tr>
<td>Unauthorised Access</td>
</tr>
<tr>
<td>Failure to protect Assets &amp; Infrastructure</td>
</tr>
<tr>
<td>External Fraud</td>
</tr>
<tr>
<td>Service disruption due to external attacks</td>
</tr>
<tr>
<td><strong>External Malicious Technology Service Disruption</strong></td>
</tr>
<tr>
<td>External attacks on HIS assets</td>
</tr>
<tr>
<td>Misuse of security managed data</td>
</tr>
<tr>
<td>Customer and enterprise impacts as a result of external attacks</td>
</tr>
<tr>
<td>Inability to operate in disaster scenario</td>
</tr>
<tr>
<td>Category</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Information Systems Failure</td>
</tr>
<tr>
<td><strong>External Theft from Customer Accounts</strong></td>
</tr>
<tr>
<td>External fraudulent activity</td>
</tr>
<tr>
<td>Third Party external fraud committed</td>
</tr>
<tr>
<td>External Fraud from external party or client generated instruction</td>
</tr>
<tr>
<td><strong>External Theft from Group Company Accounts</strong></td>
</tr>
<tr>
<td>External Fraud Risk</td>
</tr>
<tr>
<td>External Theft from Group Company Accounts</td>
</tr>
<tr>
<td>Failure to identify and protect against evolving landscape of cyber threats in a timely manner</td>
</tr>
<tr>
<td>Lost/stolen large value cheques</td>
</tr>
<tr>
<td><strong>External Theft of Information</strong></td>
</tr>
<tr>
<td>External Theft of Information</td>
</tr>
<tr>
<td>Theft of information from external party</td>
</tr>
<tr>
<td><strong>External Vendor or Service Provider Breach of Contract</strong></td>
</tr>
<tr>
<td>Counterparty fails to receive and/or send orders</td>
</tr>
<tr>
<td>Failure to govern and realise the value of end-to-end management of Third-Party Suppliers (EST risk)</td>
</tr>
<tr>
<td><strong>Failed or Inaccurate Reporting</strong></td>
</tr>
<tr>
<td>External Reporting Failure Risk</td>
</tr>
<tr>
<td>Inaccurate or Untimely Submission of Regulatory Reporting</td>
</tr>
<tr>
<td>Failed or Inaccurate Reporting</td>
</tr>
<tr>
<td>Inability to Leverage Enterprise Data</td>
</tr>
<tr>
<td><strong>Health &amp; Safety of Employees or Third Parties Failure</strong></td>
</tr>
<tr>
<td>Health &amp; Safety of Employees or Third Parties Failure</td>
</tr>
<tr>
<td>Failure to respond to workplace incidents</td>
</tr>
<tr>
<td>Occupational Health &amp; Safety</td>
</tr>
<tr>
<td><strong>Inadequate Advisory Activities</strong></td>
</tr>
<tr>
<td>Inadequate Advisory Activities (Secretariat Function)</td>
</tr>
<tr>
<td>Inadequate Advisory Activities (training)</td>
</tr>
<tr>
<td>Adequate levels of suitably skilled staff</td>
</tr>
<tr>
<td>Skill Sets</td>
</tr>
<tr>
<td><strong>Inadequate Client Disclosures</strong></td>
</tr>
<tr>
<td>Disclosure of required information</td>
</tr>
<tr>
<td>Communications to customers</td>
</tr>
<tr>
<td>Failure to deliver cards services on time/qual</td>
</tr>
<tr>
<td><strong>Inadequate Client Investigation (KYC - Know Your Customer)</strong></td>
</tr>
<tr>
<td>Risk of money laundering via branch</td>
</tr>
<tr>
<td>AML / KYC</td>
</tr>
<tr>
<td>AML/CTF compliance</td>
</tr>
<tr>
<td><strong>Inadequate Client Management</strong></td>
</tr>
<tr>
<td>Insufficient Scanning Algorithms</td>
</tr>
<tr>
<td>Strategy &amp; Reporting</td>
</tr>
<tr>
<td>Failure to maintain a current OFAC db</td>
</tr>
<tr>
<td>Category</td>
</tr>
<tr>
<td>---------------------------------------</td>
</tr>
<tr>
<td>Change Management Failure</td>
</tr>
<tr>
<td>Incorrect Credit Listing</td>
</tr>
<tr>
<td>Cash Activities</td>
</tr>
<tr>
<td>Inadequate Complaints Handling</td>
</tr>
<tr>
<td>Complaints handling and dispute resolution</td>
</tr>
<tr>
<td>Complaint Handling</td>
</tr>
<tr>
<td>Inadequate complaint management</td>
</tr>
<tr>
<td>Increased litigation</td>
</tr>
<tr>
<td>Inappropriate Contractual Terms</td>
</tr>
<tr>
<td>Misunderstanding and categorisation of RMCs</td>
</tr>
<tr>
<td>Incorrect or Poor Credit Decisions</td>
</tr>
<tr>
<td>Incomplete Client Documents</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Incomplete Client Records</td>
</tr>
<tr>
<td>Insider Trading (for personal gain)</td>
</tr>
<tr>
<td>Insider Trading/Conflict of Interest</td>
</tr>
<tr>
<td>Insider Trading (for personal gain)</td>
</tr>
<tr>
<td>General Regulatory Compliance Failure</td>
</tr>
<tr>
<td>Insider Trading</td>
</tr>
<tr>
<td>Insider Trading/Conflicts Interest</td>
</tr>
<tr>
<td>Internal e-Fraud</td>
</tr>
<tr>
<td>Lost or Missing Client Documents</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Malicious Destruction of Assets by Employees</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Market Misconduct</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Missed External Deadline or Responsibility</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Missed Internal Deadline or Responsibility</td>
</tr>
<tr>
<td>(PROPOSED DIVISIONAL RISK) Regulatory Change Implementation Failure</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>Inability to meet internal colleague service requirements</td>
</tr>
<tr>
<td>Change Delivery &amp; Implementation failure (including CSR)</td>
</tr>
<tr>
<td>Failure to deliver and effectively embed change in line with the defined business case resulting in benefits &amp; outcomes not being realised</td>
</tr>
<tr>
<td>Failure to execute business activities</td>
</tr>
</tbody>
</table>

**Mis-selling**
- Provision of advice or incorrect information via telephone

**MIS-SELLING**

**Misuse of Confidential Information**
- Misuse of Confidential Information
- Misuse of Customer Information
- Leakage and Misuse of Confidential Information
- Confidentiality / Data Protection Breach
- Privacy Breaches

**Model or System Failure**
- Model Error
- Insufficient workforce agility
- Workforce Agility
- Insufficient Workforce Agility

**Money Laundering**
- Noncompliance with Global AML/CTF Regulations
- Regulatory Compliance Breach (Operations US)
- Non adherence to AML / Sanctions legislation
- Failure to report Suspicious Activity
- Failure to satisfy AML requirements
- Inadequate Client AML-KYC applications and PEPs/Sanctions Screening
- Non-adherence to Regulatory Obligations

**Poor Vendor Performance**
- Poor Vendor Performance
- Poor Vendor Performance
- Poor Vendor Performance

**Product Design Flaws Excluding Contractual Terms**
- System apps not supported by Technology
- Change not implemented within risk framework

**Unauthorised Transaction Activity by Employees**
- Internal Fraud
- Financial Impact due to Internal Fraud
- Internal and/or external fraud
- Risk of Excessive System Access Rights
- Loss of commercially sensitive information
- Unauthorised Transaction Activity by Employees
- Fraud
- CHNB-Corruption Risk associated with bribery
<table>
<thead>
<tr>
<th><strong>Office Account Management</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Fraud</td>
</tr>
<tr>
<td>Risk of Lost or Stolen cash and Valuables</td>
</tr>
<tr>
<td>Insider Trading/Fraud</td>
</tr>
<tr>
<td>Violation</td>
</tr>
<tr>
<td>Theft of Confidential Information</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Unlicensed Activity</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Unlicensed Activity</td>
</tr>
<tr>
<td>Unlicensed Activity</td>
</tr>
<tr>
<td>Regulatory Compliance Breaches</td>
</tr>
</tbody>
</table>
Appendix D: Participant interview exhibits to elicit current state causes and effects
ITRM

Technology, Cust. Payments & Process
Shared Services & Bus Mgt.
Customer Services
Enterprise Projects

Risk Category

Operational
Compliance
Customer Fairness & Conduct
Regulatory

Significant Business Disruption
Mis-selling of Lending, Transactional and Insurance Products
Ineffective Delivery
Non Compliance with APRA/ASIC
Data Quality and Transaction Capture Errors
External Risk
Internal Fraud
Risk Types

Operational Risk
- Anti-Fraud
- Business Continuity Management
- Event Management
- Information Security
- Model Risk
- Operational Risk Profiling
- Outsourcing and Offshoring
- Physical Security
- Travel Security
- Environment

Compliance Risk
- Anti-Bribery and Corruption
- Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF)
- Compliance risk management framework
- Licence management standard
- Enforced Conduct Policy (in reference to the Code of Conduct)
- Conflicts of Interest
- Environmental Management
- Environmental Operating Reporting and Offset Management
- Privacy and Data Protection
- Sanctions and Embargoes

Customer
- Customer Complaints
- Customer Privacy
- Customer Safety
- Customer Equal Treatment
Appendix E: Interview Data Process Map Example
Appendix F: Ethics Approval

Notice of Approval

Date: 2 July 2015
Project number: 19204
Project title: Financial Supply Chain Risk and Australia Financial Institutions’ Performance
Risk classification: Low risk
Principal Investigator:
Student Investigator:
Other Investigator:
Project Approved: From: 30 June 2015 To: 6 October 2020
Terms of approval:

Responsibilities of the principal investigator

It is the responsibility of the principal investigator to ensure that all other investigators and staff on a project are aware of the terms of approval and to ensure that the project is conducted as approved by BCHEAN. Approval is only valid while the investigator holds a position at RMIT University.

1. Amendments
   Approval must be sought from BCHEAN to amend any aspect of a project including approved documents. To apply for an amendment submit a request for amendment form to the BCHEAN secretary. This form is available on the Human Research Ethics Committee (HREC) website. Amendments must not be implemented without first gaining approval from BCHEAN.

2. Adverse events
   You should notify BCHEAN immediately of any serious or unexpected adverse effects on participants or unforeseen events affecting the ethical acceptability of the project.

3. Participant Information and Consent Form (PICF)
   The PICF must be distributed to all research participants, where relevant, and the consent form is to be retained and stored by the investigator. The PICF must contain the RMIT University logo and a complaints clause including the above project number.

4. Annual reports
   Continued approval of this project is dependent on the submission of an annual report.

5. Final report
   A final report must be provided at the conclusion of the project. BCHEAN must be notified if the project is discontinued before the expected date of completion.

6. Monitoring
   Projects may be subject to an audit or any other form of monitoring by BCHEAN at any time.

7. Retention and storage of data
   The investigator is responsible for the storage and retention of original data pertaining to a project for a minimum period of five years.

Regards,
Appendix G: Letter to Participants

8-Oct-19

Dear Sir/Madam,

As an expert in the field we wish to invite you to participate in this research that is of considerable relevance to your senior risk managerial role in your Financial Institution.

This PhD project will investigate the relationship between financial supply chain risks and the performance of the Financial Institutions in Australia. The objective of this research is to develop a conceptual model for the determinants affecting financial supply chain risks (FSCRs) and to examine their impact on the performance of financial institutions in the context of Australia. It will be a qualitative research study collecting information by interviewing senior risk managers specialized in this field. The interview questions will address the causes of financial supply chain risks and its impact on the Financial Institutions’ performance. The research outcomes will help managers to understand the critical determinants that contribute to financial supply chain risks and develop strategies that managers can use to eradicate and combat risks in the financial supply chain.

We are approaching two senior risk managers from your Financial Institution to gather information given their expert knowledge in risk division in the financial industry in Australia.

The academic investigators in this project include:

- 
- 
- 

The anticipated outcomes of the research will include a thesis, journal articles, a student report or presentation at conferences on issues likely to include:
- To examine the interrelationship between Financial Supply Chain Risks (FSCRs) and Performance of the Financial Institution;
- To assist entrepreneurs and business people to be acquainted with the knowledge about the products in the supply chain of financial institutions in Australia.

If you are agreeable to an interview, we would ask if your comments can be recorded in response to questions posed by Mr. [Name] for further analysis. If you do not wish the interview to be recorded Mr. [Name] is quite willing to take notes. The interview may take a maximum of one hour. All the names of people interviewed will remain anonymous, pseudonyms will be used at all times and the financial institute you represent will not be linked specifically to any individual comments recorded or reproduced in research publications. All data will only be accessible to the three investigators and will be stored on the password protected server at RMIT. The research data will be kept securely at RMIT for 5 years and then destroyed.

The benefits of this research will include providing you with a summary of comments made by your colleagues, again maintaining strict anonymity in compliance with RMIT’s ethics committee which has approved this research. Any publications, including the thesis will be made accessible to you as a courtesy. No harm is foreseen as a result of your participation in this research, however you have the right to decline to participate and to withdraw from the research without any consequences as this is a key aspect of the RMIT ethics practices that we respect.
In summary your rights as a participant include:

- The right to withdraw from participation at any time
- The right to request that any recording cease
- The right to have any unprocessed data withdrawn and destroyed, provided it can be reliably identified, and provided that so doing does not increase the risk for you as the participant.
- The right to have any questions answered at any time.

In the event that you have any concerns or questions at any time please contact the senior supervisor - Professor [Name] - and his contact details are listed above.

Mr Abdallah will contact you to arrange a time to interview you hoping you are amenable to participating in this research. In the event that you kindly agree to participate Mr Abdallah will ask you to sign the attached consent form that will be provided at the interview.

Thank you for considering our request.

Yours sincerely

If you have any concerns about your participation in this project, which you do not wish to discuss with the researchers, then you can contact the Ethics Officer, Research Integrity, Governance and Systems, RMIT University, GPO Box 2476V VIC 3001. Tel: (03) 9925 2251 or email human.ethics@rmit.edu.au
Participant Consent Form

1. I have had the project explained to me, and I have read the information sheet

2. I agree to participate in the research project as described

3. I agree:
   - to be interviewed
   - that my voice will be audio recorded

4. I acknowledge that:
   (a) I understand that my participation is voluntary and that I am free to withdraw from the project at any time and to withdraw any unprocessed data previously supplied (unless follow-up is needed for safety).
   (b) The project is for the purpose of research. It may not be of direct benefit to me.
   (c) The privacy of the personal information I provide will be safeguarded and only disclosed where I have consented to the disclosure or as required by law.
   (d) The security of the research data will be protected during and after completion of the study. The data collected during the study may be published, and a report of the project outcomes may be provided in a thesis, journal articles, at conferences, and student presentations but any information which will identify me will not be used.

Participant’s Consent

Participant: _______________________ Date: ______________________

(Signature)

As a participant you will be provided with a photocopy of this form after it has been signed by you.