Exploring the business benefits of regulatory compliance: the case of AML/CFT systems for banking institutions in Malaysia

Additional Information:

- A Doctoral Thesis. Submitted in partial fulfilment of the requirements for the award of Doctor of Philosophy of Loughborough University.

Metadata Record: https://dspace.lboro.ac.uk/2134/12362

Publisher: © Abdullah Othman

Please cite the published version.
This item was submitted to Loughborough University as a PhD thesis by the author and is made available in the Institutional Repository (https://dspace.lboro.ac.uk/) under the following Creative Commons Licence conditions.

For the full text of this licence, please go to:
http://creativecommons.org/licenses/by-nc-nd/2.5/
Exploring the Business Benefits of Regulatory Compliance: The case of AML/CFT systems for banking institutions in Malaysia

by

Abdullah Othman

A Doctoral Thesis

Submitted in partial fulfilment of the requirements for the award of the degree of Doctor Philosophy of Loughborough University

March 2013

© by Abdullah Othman, 2013
Acknowledgements

A long and challenging journey starts with the first step. And indeed I am glad that I have taken that very first step, now seemed quite a while back, towards this journey to pursue my utmost ambition. Even though I must admit that it has not been all wonderful, the journey has nevertheless been a rewarding experience; positively challenging; mind stimulating; and importantly, has given me the opportunity to be in overall, a better person. And now since I am reaching the few final steps of my journey, I would like to take the opportunity to express my sincere appreciation and gratitude to those individuals and parties that have been very instrumental and influential in their role towards the completion of this research.

My deepest appreciation goes to Professor Neil F. Doherty, my supervisor, for his continuous guidance; unwavering support; encouragement; and patience towards me throughout this journey. Also to my employer and sponsor, Bank Negara Malaysia (i.e. the Central Bank of Malaysia), for their financial assistance and allowing me to pursue this ambition. Not forgetting, to the selected professionals and leaders of banking institutions in Malaysia, as well as the central bankers, for their willingness to participate in this research; providing valuable insights; and allowing me to leverage their knowledge and experience.

Last but not least, to my wife, Fauziah, for the love and understanding during those difficult and challenging times, and for someone to share the joy with during the moment of celebrations and jubilations. Also to my three sons; Amir, Afiq and Aqif; thank you for the ever humorously cheeky and mischievous requests. They certainly keep reminding me about the joys and happiness of parenthood, and importantly the life that will always awaits me beyond this journey that I have undertaken.

This thesis is especially dedicated to my mum, for her comforting words and moral support; and also to my dad and my adopted parents, who did not lived to see this.

Abdullah Othman
March 2013
Abstract

It has been widely accepted that the banking industry is highly dependent on information technology (IT). Due to its pervasiveness and intertwining nature in most aspects of banking business, IT has also significantly become one of the critical components that facilitate the ability of banking institutions to meet regulatory requirements in an efficient and a cost-effective way. For instance, in the effort to mitigate the activities of money laundering and terrorism financing (ML/TF), various information on banking customers are timely and accurately gathered and analysed through automation. Furthermore, in many instances, IT systems exclusively built to achieve a similar objective are frequently established, and comparable to most IT implementations in the banking institutions, they are often can be equally regarded as a significant investment as well.

Viewed from the longstanding debate on the value of IT investments to organisations, empirical research within the IS domain seemed to have placed less emphasis on the possible contribution of regulatory IT implementations. While it is easy to conceive that these IT deployments were never intended to directly benefit banking business from the outset, a study from this perspective should not be disregarded, but instead, warrant to be equally explored. The rationale for this statement can be attributed to the aforementioned assertion regarding the potentially substantial monetary investments required. In addition to this, it may also be due to the high tendency of stringent regulations being enforced in the future, and hence, could inevitably place a significant demand on organisational resources, and further influence their associated opportunity costs.

For that reason, this study has attempted to fill the identified research gaps by conducting an investigation from the standpoint of a topical issue regarding anti-money laundering and counter terrorism financing (AML/CFT) implementation efforts within banking institutions. Utilising a conceptual framework that leverages the resource-based view (RBV) to structurally analyse a list of research objectives, empirical evidence of business benefits and the associated capabilities through organisational AML/CFT efforts have indeed been discovered. The benefits are particularly in the form of having the opportunity to leverage various information and infrastructure that were established for regulatory purposes. Further evidence has also suggested that selected AML/CFT alerts have the potential of providing unique opportunity for the organisation to trigger time-critical event-based marketing activities, resulting in a possible improved competitive positioning (ICP). Importantly, by appreciating the insights obtained through the research, a conceptual framework is proposed, which may aid to structurally assess the possible benefits of any organisational regulatory IT implementations.
Table of Contents

1. INTRODUCTION .................................................................................................................. 1
   1.1. INTRODUCTION ........................................................................................................... 1
   1.2. DRIVERS FOR THE RESEARCH .............................................................................. 1
   1.3. SIGNIFICANCE OF THE RESEARCH ...................................................................... 3
   1.4. BROAD RESEARCH OBJECTIVES ......................................................................... 5
   1.5. OVERALL RESEARCH APPROACH .......................................................................... 6
   1.6. STRUCTURE OF THE THESIS .................................................................................... 7
   1.7. CONCLUDING REMARKS ......................................................................................... 9

2. LITERATURE REVIEW ........................................................................................................... 10
   2.1. INTRODUCTION .......................................................................................................... 10
   2.2. IT IN ORGANISATIONS ............................................................................................. 11
   2.3. IT INVESTMENT VALUE ............................................................................................ 12
   2.3.1. Common Interest on IT Value .............................................................................. 12
   2.3.2. Inconclusiveness of Findings on IT Value .......................................................... 13
   2.3.3. The Resource-Based View and IT Value ............................................................... 15
   2.4. IT AND REGULATORY COMPLIANCE .................................................................. 17
   2.4.1. Significance of Regulatory Compliance ............................................................... 17
   2.4.2. Common Standpoint on Regulatory Compliance ............................................... 18
   2.4.3. Role of IT in Regulatory Compliance ................................................................ 19
   2.4.4. Alternative Approach to Regulatory Compliance .............................................. 21
   2.5. CONCLUDING REMARKS ....................................................................................... 27

3. RESEARCH OBJECTIVES AND FRAMEWORK ............................................................... 28
   3.1. INTRODUCTION .......................................................................................................... 28
   3.2. CRITIQUE OF EXISTING LITERATURE .................................................................. 28
   3.3. RESEARCH OBJECTIVES ......................................................................................... 31
   3.3.1. Value from Basic Compliance Activities ......................................................... 33
   3.3.2. Value from Broader Compliance Activities ....................................................... 34
   3.3.3. Role of IS Capabilities in Facilitating Value ...................................................... 36
   3.3.4. Impact on Competitive Positioning ..................................................................... 36
   3.4. CONCEPTUAL RESEARCH FRAMEWORK ............................................................. 37
   3.4.1. Potential Relationships ....................................................................................... 37
   3.4.2. IS Capabilities for Regulatory Requirements .................................................... 40
   3.4.3. Attributes of Competitive Positioning ................................................................. 45
   3.5. CONCLUDING REMARKS ....................................................................................... 47

4. RESEARCH STRATEGY, DESIGN AND METHODOLOGY ............................................. 48
   4.1. INTRODUCTION .......................................................................................................... 48
   4.2. PHILOSOPHICAL STANDPOINT ............................................................................. 49
   4.3. RESEARCH STRATEGY ............................................................................................. 50
   4.3.1. Qualitative Versus Quantitative ........................................................................ 50
   4.4. RESEARCH DESIGN ................................................................................................. 54
   4.4.1. Rationale for the Adopted Research Design ....................................................... 54
   4.4.2. Quality Criteria for Qualitative Research .......................................................... 58
   4.5. RESEARCH METHODOLOGY ................................................................................ 60
4.5.1. Gathering and Sampling of Data .............................................. 61
4.5.2. Analysis of Data ......................................................................... 64
4.5.3. Location of Study ......................................................................... 66
4.6. CONSTRAINTS AND LIMITATIONS .................................................. 67
4.7. ETHICAL CONSIDERATIONS .......................................................... 70
4.8. CONCLUDING REMARKS .............................................................. 71

5. DATA GATHERING, INITIAL ANALYSIS AND BACKGROUND .......... 73

5.1. INTRODUCTION ............................................................................ 73
5.2. DATA GATHERING ........................................................................ 74
  5.2.1. Pilot Interviews ........................................................................ 74
  5.2.2. First Phase Interviews ................................................................. 75
  5.2.3. Second Phase Interviews .............................................................. 82
  5.2.4. Supplementary Interviews ......................................................... 89
5.3. DATA ANALYSIS ............................................................................ 90
5.4. PRESENTATION OF INITIAL FINDINGS ........................................... 92
  5.4.1. Preliminary Findings Against Research Objectives ......................... 93
  5.4.2. Motivation for Focusing on AML/CFT ......................................... 99
  5.4.3. Justifications for Adopting an Individual IS Orientation ................ 101
  5.4.4. Rationale for Concentrating on Detailed Case Studies .................. 102
5.5. CONTEXTUAL BACKGROUND ......................................................... 105
  5.5.1. Background of AML/CFT Regulatory Requirements .................... 106
  5.5.2. Key AML/CFT Requirements for the Banking Industry .................. 111
  5.5.3. Primary Components of an AML/CFT IT System .......................... 113
  5.5.4. Background on Detailed Case Studies’ AML/CFT IT Systems ......... 115
  5.5.5. Overall Assumption and Approach in Detailed Data Analysis ........ 120
5.6. CONCLUDING REMARKS .............................................................. 122

6. ANALYSIS OF COMPLIANCE BENEFITS ........................................ 123

6.1. INTRODUCTION ............................................................................ 123
  6.1.1. Analytical Approach .................................................................. 124
  6.1.2. Underlying Information Architecture .......................................... 126
  6.1.3. Identified Categories of Compliance Benefits .............................. 128
6.2. CUSTOMER VERIFICATION BENEFITS ......................................... 129
  6.2.1. Customer Validation ................................................................. 130
  6.2.2. Information Reliability ............................................................... 133
  6.2.3. Termination of Business Relationships ....................................... 135
6.3. CUSTOMER MONITORING BENEFITS ........................................ 137
  6.3.1. Discrepancies in Financial Transactions ...................................... 137
  6.3.2. Customer Risk Profiling ............................................................. 140
  6.3.3. Violations in Threshold Limits .................................................. 143
  6.3.4. Politically Related Customers ................................................... 145
  6.3.5. Customers from Countries Under Observation ............................. 147
  6.3.6. Matching of Names Under Surveillance ...................................... 148
6.4. CUSTOMER CATEGORISATION BENEFITS .................................. 150
  6.4.1. Differential Engagement Strategy .............................................. 151
6.5. COMPUTERISATION BENEFITS ..................................................... 153
  6.5.1. Management Information System .............................................. 153
6.6. REPUTATIONAL BENEFITS ............................................................ 157
  6.6.1. Effectiveness in Monitoring and Detection .................................. 158
  6.6.2. Mitigation of Regulatory Penalties ............................................. 158

Page v
9.3.2. Contribution in the Form of a Revised Framework ............................ 295
9.4. RESEARCH IMPLICATIONS ................................................................. 305
  9.4.1. Managerial Implications ............................................................. 305
9.5. PERSONAL REFLECTIONS ................................................................. 306
9.6. LIMITATIONS OF THE STUDY .......................................................... 308
9.7. OPPORTUNITIES FOR FUTURE RESEARCH ...................................... 309
9.8. CONCLUDING REMARKS ................................................................. 310

List of References ....................................................................................... 311
List of Appendices ....................................................................................... 328
List of Tables

Table 3-1: Identified Gaps in Comparison to Research Objectives ........................................... 33
Table 3-2: IS Capabilities – Original and Adopted Definitions ................................................. 42
Table 5-1: Interview List – First Phase ...................................................................................... 82
Table 5-2: Interview List – Second Phase .................................................................................. 88
Table 5-3: Interview List – Supplementary .............................................................................. 89
Table 6-1: Benefit of Validating Customers .............................................................................. 132
Table 6-2: Benefit of Information Reliability and Up-to-dateness ............................................. 134
Table 6-3: Benefit of Terminating Business Relationship ....................................................... 136
Table 6-4: Benefit of Discovering Discrepancies in Financial Transactions .............................. 139
Table 6-5: Benefit of Monitoring Customer Risk Profiling ...................................................... 142
Table 6-6: Benefit of Detecting Violations in Threshold Limits ............................................... 144
Table 6-7: Benefit of Monitoring Politically Exposed Persons ................................................. 146
Table 6-8: Benefit of Detecting Customers from Countries Under Observation ...................... 148
Table 6-9: Benefit of Matching of Names Under Surveillance ............................................... 150
Table 6-10: Benefit of Implementing Differential Engagement Strategy ................................. 152
Table 6-11: Benefit of Establishing Management Information System .................................. 157
Table 7-1: Benefit of Leveraging Identification and Background Information ........................... 173
Table 7-2: Benefit of Leveraging Riskiness Information ......................................................... 178
Table 7-3: Benefit of Leveraging the Opportunity to be Selective .......................................... 183
Table 7-4: Benefit of Leveraging Fraud Functionalities ........................................................... 189
Table 7-5: Benefit of Leveraging Regulatory IT Repository ..................................................... 200
Table 7-6: Benefit of Leveraging Time-critical Event-based Information ............................... 221
Table 8-1: Business Advantages of ERM Capability ............................................................... 263
Table 8-2: Business Advantages of ISI Capability ................................................................. 266
Table 8-3: Business Advantages of CEISO Capability ............................................................ 268
Table 8-4: Business Advantages of CBP Capability ............................................................... 273
Table 8-5: Business Advantages of BK Capability ................................................................. 275
Table 8-6: Business Advantages of AIS Capability ............................................................... 277
List of Figures

Figure 1-1: The Thesis Structure ................................................................................................... 8
Figure 3-1: The Conceptual Research Framework .......................................................................... 38
Figure 5-1: AML/CFT Analysis of Transactional Information ......................................................... 119
Figure 7-1: Relationships - Compliance and Supplementary Benefits .............................................. 165
Figure 8-1: Capabilities Associated with Compliance Benefits ......................................................... 227
Figure 8-2: General Relationships - Capabilities and Compliance Benefits .................................... 227
Figure 8-3: Key Stakeholders in the AML/CFT Implementation .......................................................... 230
Figure 8-4: Relationships - Department, Stage, Capability & Compliance Benefits ....................... 256
Figure 8-5: Extended Usage of Capabilities Facilitating Supplementary Benefits ............................ 279
Figure 8-6: Relationships - Department, Stage, Capability & Supplementary Benefits ................. 280
Figure 9-1: Key Phases for Framework Creation ............................................................................... 296
Figure 9-2: Framework on Assessing Business Benefits of Mandatory IT Implementations ... 297
## List of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIS</td>
<td>Analytical and Investigation Skills</td>
</tr>
<tr>
<td>AML/CFT</td>
<td>Anti-Money Laundering and Counter Financing of Terrorism</td>
</tr>
<tr>
<td>AMLATFA</td>
<td>Anti-Money Laundering and Anti-Terrorism Financing Act (2001)</td>
</tr>
<tr>
<td>ATM</td>
<td>Automated Teller Machine</td>
</tr>
<tr>
<td>AVP</td>
<td>Assistant Vice President</td>
</tr>
<tr>
<td>BAFIA</td>
<td>Banking and Financial Institutions Act (1989)</td>
</tr>
<tr>
<td>BBC</td>
<td>British Broadcasting Corporation</td>
</tr>
<tr>
<td>BCBS</td>
<td>Basel Committee on Banking Supervision</td>
</tr>
<tr>
<td>BK</td>
<td>Business Knowledge</td>
</tr>
<tr>
<td>CAAR</td>
<td>Customer Account Aggregated Risk</td>
</tr>
<tr>
<td>CAQDAS</td>
<td>Computer-Assisted/Aided Qualitative Data Analysis</td>
</tr>
<tr>
<td>CBA</td>
<td>Cost-benefit Analysis</td>
</tr>
<tr>
<td>CBP</td>
<td>Compliance-Business Partnerships</td>
</tr>
<tr>
<td>CCR</td>
<td>Customer Core Risk</td>
</tr>
<tr>
<td>CCRIS</td>
<td>Central Credit Reference Information System</td>
</tr>
<tr>
<td>CDD</td>
<td>Customer Due Diligence</td>
</tr>
<tr>
<td>CEISO</td>
<td>Cost-Effective IS Operations</td>
</tr>
<tr>
<td>CEO</td>
<td>Chief Executive Officer</td>
</tr>
<tr>
<td>CER</td>
<td>Customer Effective Risk</td>
</tr>
<tr>
<td>CFO</td>
<td>Chief Financial Officer</td>
</tr>
<tr>
<td>CIO</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>CONG</td>
<td>Compliance Officers Networking Group</td>
</tr>
<tr>
<td>COO</td>
<td>Chief Operating Officer</td>
</tr>
<tr>
<td>CRM</td>
<td>Customer Relationship Management</td>
</tr>
<tr>
<td>CTR</td>
<td>Cash Transaction Report</td>
</tr>
<tr>
<td>EDI</td>
<td>Electronic Data Interchange</td>
</tr>
<tr>
<td>EDW</td>
<td>Enterprise Data Warehouse</td>
</tr>
<tr>
<td>ERM</td>
<td>External Relationship Management</td>
</tr>
<tr>
<td>ETL</td>
<td>Extract, Transform, and Load</td>
</tr>
<tr>
<td>FATF</td>
<td>The Financial Action Task Force</td>
</tr>
<tr>
<td>FIU</td>
<td>Financial Intelligence Unit</td>
</tr>
<tr>
<td>GDW</td>
<td>Group Data Warehouse</td>
</tr>
<tr>
<td>HIPAA</td>
<td>The Health Insurance Portability and Accountability Act (1996)</td>
</tr>
<tr>
<td>IAIS</td>
<td>International Association of Insurance Supervisors</td>
</tr>
<tr>
<td>ICP</td>
<td>Improved Competitive Positioning</td>
</tr>
<tr>
<td>IOSCO</td>
<td>International Organization of Securities Commission</td>
</tr>
<tr>
<td>Acronym</td>
<td>Acronym Full Form</td>
</tr>
<tr>
<td>---------</td>
<td>------------------</td>
</tr>
<tr>
<td>IS</td>
<td>Information System</td>
</tr>
<tr>
<td>ISBP</td>
<td>IS-Business Partnerships</td>
</tr>
<tr>
<td>ISD</td>
<td>IS Development</td>
</tr>
<tr>
<td>ISI</td>
<td>IS Infrastructure</td>
</tr>
<tr>
<td>ISPCM</td>
<td>IS Planning and Change Management</td>
</tr>
<tr>
<td>ISTS</td>
<td>IS Technical Skills</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>KYC</td>
<td>Know Your Customer</td>
</tr>
<tr>
<td>MIS</td>
<td>Management Information System</td>
</tr>
<tr>
<td>ML/TF</td>
<td>Money Laundering and Terrorism Financing</td>
</tr>
<tr>
<td>MR</td>
<td>Market Responsiveness</td>
</tr>
<tr>
<td>NPL</td>
<td>Non-Performing Loan</td>
</tr>
<tr>
<td>NRIC</td>
<td>National Registration Identity Card</td>
</tr>
<tr>
<td>OFAC</td>
<td>The Office of Foreign Assets Control</td>
</tr>
<tr>
<td>PEP</td>
<td>Politically Exposed Person</td>
</tr>
<tr>
<td>RBV</td>
<td>Resourced-based View</td>
</tr>
<tr>
<td>RM</td>
<td>Ringgit Malaysia</td>
</tr>
<tr>
<td>ROI</td>
<td>Return on Investment</td>
</tr>
<tr>
<td>SCA</td>
<td>Sustained Competitive Advantage</td>
</tr>
<tr>
<td>SCG1</td>
<td>Sectoral Guidelines 1 on AML/CFT</td>
</tr>
<tr>
<td>SEC</td>
<td>Securities and Exchange Commission</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Messaging Service</td>
</tr>
<tr>
<td>SOX</td>
<td>Sarbanes-Oxley Act (2002)</td>
</tr>
<tr>
<td>STG</td>
<td>Standard Guidelines on AML/CFT</td>
</tr>
<tr>
<td>STR</td>
<td>Suspicious Transaction Report</td>
</tr>
<tr>
<td>UAT</td>
<td>User Acceptance Testing</td>
</tr>
<tr>
<td>UN</td>
<td>The United Nations</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

1.1. INTRODUCTION

This chapter outlines the contextual background of the research. It begins by presenting the research driving factors, which briefly describes the underlying rationale for the research. This is then followed by the discussion on the significance of the research; the general research objectives; as well as the overall research approach. The overall structure of the thesis is also presented, before the chapter is summarised and brought to close by the concluding remarks section.

1.2. DRIVERS FOR THE RESEARCH

It has been generally accepted that IT is significant to organisations, in terms of its usage and its share of the total investment. The annual IT investment (i.e. computer, office and communication equipment, not including software and systems development cost) by industries in the United States is reported to be hundreds of billions of dollars (Barua et al., 1995), and studies have shown that about one-third of all capital spending is in the area of IT (Parent and Reich, 2009, Bakos, 1998). Focusing specifically on the financial industry, financial institutions are seen to be particularly dependent on IT. The industry has among the largest investment relating to IT, mainly attributed to the digital characteristics of its products and services (Berger, 2003, De Haes and Van Grembergen, 2008, Ray et al., 2005). As IT is increasingly vital to the business, determining the value derived from this substantial IT investment has continuously attracted the interest of researchers within the IS domain (e.g. Chau et al., 2007, Ward et al., 1996, Melville et al., 2004).
Besides IT pervasiveness, another important aspect that is significantly affecting the financial institutions is the need to comply with various requirements imposed by the regulatory authorities. It has been widely acknowledged as well that the financial industry is often regarded as one of the most heavily regulated industries (e.g. Fisher and Harindranath, 2004, Garcia, 2004). Interestingly, arising from the heavy usage of IT in financial institutions, IT has also been considered as one of the critical enablers to ensure that requirements are effectively and efficiently met (e.g. Damianides, 2006, Lurie, 2004). On many occasions, although generally not made obligatory, IT systems solely for the purpose of regulatory compliance (such as used for detecting and mitigating money laundering and terrorism financing activities [ML/TF]) are often established. Furthermore, as compared to the general IT implementations for business purposes within the financial institutions, these systems are frequently regarded as a significant investment as well.

Regulatory compliance is commonly viewed as a cost of doing business that generally burdens the organisation (e.g. Walter and Rolf, 2005, Raghavan, 2007, Elliehausen, 1998). However, some conceptual literature has drawn attention to the possibility of leveraging regulatory requirements to provide opportunities for business improvement (Garcia, 2004, Volonino et al., 2004, Wagner and Dittmar, 2006). Nevertheless, empirical research within the IS domain relating to the continuing debate on value of IT investments, thus far, seems to have placed less emphasis on the potential contribution of regulatory system implementations. In this regard, little research has been conducted, within the field of IS, that has empirically explored and provided sufficient understanding of the possibility of attaining benefits from regulatory compliance activities. Importantly, it has also yet to provide useful insights into the possibility of organisations leveraging these compliance activities as an opportunity to directly benefit their business, by exploring other activities, considerations or changes that are beyond mere regulatory compliance.

It is sensible to consider that regulatory IT implementations are typically not intended to directly benefit organisation’s business or improve organisational revenue. Nevertheless, the significant role of financial institutions’ IT systems used to gather, process and produce the required regulatory information especially relating to their
customers, may warrant to be explored and appreciated from the perspective of business benefits. Furthermore, since regulatory requirements are hardly ever revoked, and new ones continue to be endorsed (Elliehausen, 1998), it might be essential for organisations to view compliance activities as an opportunity to directly enhance the value to business. The prospect of more stringent regulatory requirements to be implemented may inevitably place a substantial demand on the already stretched organisational resources, and further influenced their associated opportunity costs.

Therefore, given the high dependency on IT for regulatory compliance, as well as knowing that implementation of regulatory IT systems is mostly inevitable, the notion that such projects could be leveraged for wider business benefit merits further consideration. In exploring this possibility, the research will primarily be focusing on IT implementations that are developed for regulatory purposes. Furthermore, the nature of value that would be of interest to this research will not only be limited to the attainable benefits from directly complying with regulatory requirements and meeting the expected deliverables. Rather, this research will attempt to further explore and appreciate the associated gains and advantages that could possibly be achieved from efforts to broaden the fundamental regulatory compliance activities and positively influence banking business.

1.3. SIGNIFICANCE OF THE RESEARCH

This research offers important insights into the implementation of regulatory compliance IT systems and the possibility of attaining benefits from meeting the expected deliverables, and importantly, their potential in enabling direct business benefits. Towards this end, the research will be primarily rooted on the longstanding concern in determining the value of organisations’ IT investments (e.g. Chau et al., 2007, Ward et al., 1996, Peppard et al., 2000, Doherty and Terry, 2009), albeit being a slight departure from the mainstream study, through its focus on regulatory IT system implementations.
There is a pressing need to gain useful insights from these distinct but significant category of organisational IT implementations that should be treated as an important source for creating value, but nevertheless has largely been ignored by IS researchers, in the past. The rationale for this line of thinking is premised on the earlier understanding on the extensive usage of IT to efficiently and effectively achieve regulatory compliance; as well as the numerous information particularly on banking customers that have been gathered, processed and produced for regulatory purposes. In addition it is also due to the potential significant monetary investments of regulatory IT implementation; as well as the prospect of more and severe future regulations being imposed (which will inevitably further add to the cost of compliance and the demands on organisational resources).

Expanding the discussion on regulatory demands, regulations can generally be considered as necessary evil that are not usually withdrawn, but instead having high propensity to be increased and be more burdening in the future (e.g. Elliehausen, 1998, Paul et al., 2008, Hüpkes and Zibung, 2008). Therefore, it is paramount for organisations to be able to comply with these requirements in a way that would bring greater good to their organisations (Garcia, 2004), and further, viewing them as an opportunity to improve, rather than predominantly observing it from a purely cost perspectives. The ability for organisations to view regulatory requirements from a different perspective could be essential, given the general understanding that they are typically being perceived as an additional cost of doing business (e.g. Elliehausen, 1998, Alfon and Andrews, 1999).

It is therefore envisaged that this research would make a significant contribution to the literature by empirically exploring the implementation and deployment of regulatory driven IT systems, and their potential to provide benefits arising from regulatory compliance and further, to directly enhance organisational performance.

Furthermore, using the resourced-based view (RBV) as the theoretical perspective, there will be another distinctive contribution aspired to be made by this research within the field of IS research. The contribution will be in the form of assessing the associated capabilities needed to efficiently and effectively achieve the numerous
regulatory objectives, expected to be delivered by organisations through their efforts to fundamentally meet regulatory requirements. Importantly, this research will likewise attempt to identify the relevant capabilities that are critical to facilitate the organisation’s ability to broaden the fundamental efforts of regulatory compliance, to provide supplementary business benefits. A comprehensive explanation on these research perspectives will be primarily presented in the following Chapter 2, with further elaborations within the chapters that follow, in line with the objectives and specific purpose of the research.

1.4. BROAD RESEARCH OBJECTIVES

This research is motivated by four broad research objectives aiming to provide important new empirical insights into organisational activities in deploying regulatory driven IT systems. These objectives can be explained as the following:

- The first research objective typically aims to appreciate banking institutions’ approaches and mechanisms for translating regulatory requirements into functional specifications, and thus meeting the expected deliverables and avoiding regulatory penalties. Therefore, this type of compliance activities tends to principally meet regulatory requirements at an acceptable level that is considered to be sufficient to avoid adverse regulatory repercussions. In addition, basic regulatory activities will only be aiming to accomplish the intended regulatory deliverables, without exploring the potential of implementing any other activities, considerations or changes that could directly be of advantage to the business. In addition, this research objective is also aiming to appreciate any instances of benefits being experienced by organisations through these basic compliance activities;

- The second research objective generally aims to discover any possible instances that can be considered as extended compliance activities. This type of activities is regarded as being achieved mainly through organisations taking deliberate efforts to implement supplementary business related activities when responding to regulatory requirements. Therefore, regulatory IT implementations can be
regarded as a catalyst to facilitate the achievement of added outcomes or objectives that directly benefit business (i.e. which are beyond the expected regulatory deliverables). These supplementary intentions can be achieved such as through incorporating extended activities, additional considerations, or optional changes within basic compliance efforts. In addition, this research objective is also aiming to obtain insights into supplementary benefits that could possibly be experienced from the deployment of these extended compliance activities;

- The third research objective typically aim to explore and understand the portfolio of IS capabilities that have assisted organisations to achieve benefits through basic compliance activities. Similarly, it is also intended to appreciate the list of IS capabilities that may possibility facilitate the achievement of benefits through extended compliance activities;

- The final research objective generally aims to gain insights into whether the attainment of benefits from basic compliance activities, and through the usage of related capabilities, have in any way positively influenced organisation’s competitive positioning. Furthermore, this research objective is also aiming to explore whether the attainment of benefits from extended compliance activities, and through the usage of relevant capabilities, have likewise provided a similar influence as well.

In a nutshell, the first and second broad research objectives aim to primarily appreciate organisations’ activities and the associated benefits in meeting compliance expectations, as well as possibly achieving additional outcomes. The last two broad research objectives, on the other hand, aimed to mainly gain insights into the capabilities required to achieve the two types of benefits, and whether they have the inclinations to influence the organisation’s competitive positioning. Detailed discussion on the research objectives, arising from these broad principles and based on a review of existing literature, will be elaborated further in Chapter 3.

1.5. OVERALL RESEARCH APPROACH

The following key stages represent the overall approach adopted by this research:
• Reviewing the extensive literature pertaining to the importance of IT to the organisations, with particular interest on the discussion regarding organisations’ IT value and the efforts to ascertain possible advantages arising from the implementation of IT solutions. In addition, reviewing the existing body of knowledge associated with organisations’ effort to meet regulatory requirements, with further concentration on the utilisation of IT to ensure efficiency and effectiveness of compliance;

• Identifying key gaps arising from the review of the literature, outlining the research objectives, and formulating the conceptual framework to empirically analyse the identified areas of interest;

• Deciding and justifying the research strategy and design to be adopted, as well as the approach in collecting research data;

• Performing the actual data collection by first conducting pilot interviews, and followed by face-to-face interview sessions conducted in several phases with member of staff in banking institutions. In addition, interviews will also be conducted with identified research participants from the regulatory authority;

• Conducting detailed analysis of the interview data, reviewing banking documentations, obtained during interviews, as well as assessing the associated regulatory requirements;

• Presenting the outcomes of the analysis and the contributions to the existing body of knowledge, as well as the introduction of an alternative approach to view the research perspectives through a revised framework.

### 1.6. STRUCTURE OF THE THESIS

This thesis is divided into nine inter-related chapters that build upon one another. A graphical representation of the overall structure of the thesis, depicting the relationship and groupings of chapters, is provided in the following Figure 1-1. A brief outline on the purpose and content for each chapter is also subsequently discussed.
Chapter 1: Introduction

- **Chapter 1 – Introduction**: provides an overview of the research through the discussion on the driving factors; the significance of the study; the general research objectives; as well as the overall research approach;
- **Chapter 2 – Literature Review**: provides a critique of existing literature focusing on the areas of IT business value and organisations’ efforts to meet regulatory requirements, which will form the theoretical foundation for the study and summarises the reasons why a study linking the two domains is desirable;
- **Chapter 3 – Research Objectives and Framework**: outlines the proposed research objectives; scoping and focus of the research; as well as followed by a presentation of the conceptual framework;
- **Chapter 4 – Research Strategy, Design and Methodology**: presents the rationalisation and justifications of the chosen research strategy; design; and data collection approach to empirically analyse the identified research objectives;
- **Chapter 5 – Data Gathering, Initial Analysis and Background**: presents the actual data collection activities, as well as findings from a preliminary analysis.
addition, it also provides the contextual background information that sets the scene for a more detailed discussion in the subsequent chapters pertaining to the analysis conducted in the research;

- Chapter 6 – Analysis of Compliance Benefits: provides analysis results pertaining to the benefits arising from organisations’ ability to meet the expected regulatory goals and objectives;
- Chapter 7 – Analysis of Supplementary Benefits: presents the outcomes of the analysis regarding the business benefits due to organisations’ ability to broaden the fundamental efforts of complying with regulatory requirements;
- Chapter 8 – Analysis of Capabilities: presents the results of the analysis on the associated capabilities to meet regulatory expectations, as well as to achieve business benefits, as well as the ability to positively influence organisation’s competitive positioning;
- Chapter 9 – Discussion and Conclusions: provides the conclusion to the thesis, by presenting the overall findings in contrast to the research objectives, and the research’s contributions to the existing body of knowledge. In addition, it also provides a presentation on a revised framework that could be utilised to alternatively view the research perspectives.

1.7. CONCLUDING REMARKS

This chapter has provided the foundation of the thesis by outlining the research background, rationale, and the approach. Most importantly, this chapter has presented the importance of the research, and justify its contributions to the existing body of knowledge. Moving forward, a detailed review of the literature will provide an assessment of existing knowledge on the value derived from IT implementations, as well as the organisations’ efforts to meet regulatory requirements imposed by regulatory authorities. The review of existing literature, which will be presented in the following chapter, will also discuss and elaborate on the possible connections between these two domains of knowledge.
2.1. INTRODUCTION

This chapter will present a detailed review of the existing body of literature that will form the theoretical foundation for this study. A review of the literature relevant to the study will ensure that the research is firmly rooted in the knowledge and insights already made available by other researchers. The reviewed literature is primarily based on journal articles, prioritising, where possible, though not necessary limited to the IS journals that are highly regarded by researchers (e.g. IS World, 2010, Willcocks et al., 2008, Fisher et al., 2007, Mylonopoulos and Theoharakis, 2001) and top management and management-related academic journals (e.g. Werner, 2002). Journal articles may generally be considered as one of the preferable sources of reference in an academic study as they commonly utilise a stringent peer-review process that ensures the quality of the published materials (Bryman, 2006, Fisher et al., 2007). However, it may be worth noting that the emphasis on peer-reviewed journals adopted by this research does not imply that other sources of reference are totally omitted. These additional sources, typically regarded as “grey literature” (Bryman, 2008) that may originate from non peer-reviewed articles and research that have been reported in book, newspaper, etc., have also been taken into consideration, where appropriate.

The process of reviewing the extant literature will use the following approach. Firstly, the overall importance of IT to the organisations will be presented. This is then followed by the discussion regarding organisations’ IT investment value and the conflicting and inconclusive nature of this domain of IS research in the attempt to ascertain possible advantages arising from the implementation of IT solutions. Furthermore, in the effort to meet regulatory requirements, the literature focusing on
the utilisation of IT to ensure efficiency and effectiveness of compliance will also be presented and discussed. Finally, the chapter will present a critical review of literature that offers the reasons and justifications as to why a study linking the two branches of knowledge is desirable and appealing.

2.2. IT IN ORGANISATIONS


Financial institutions in particular are also highly dependent on IT (Berger, 2003, De Haes and Van Grembergen, 2008), altering these institutions’ internal operations and the ways in which financial services are delivered (Pennings and Harianto, 1992). Indeed, the financial services industry has among the largest investment in IT due to the digital characteristics of its products and services (Ray et al., 2005). Through increasing competition, financial institutions are forced to implement IT to remain viable (Vitale, 1986, Lee and Bose, 2002) and to maintain current customers even though the investment may yield modest or no return (Floyd and Wooldridge, 1990, Berger, 2003). This development can be reflected in the case of automated teller
Chapter 2: Literature Review

machines (ATMs) in the 1980s, where financial institutions may have essentially ‘given away’ the benefits of the technology to their customers as the industry became more competitive (Berger, 2003). ATMs can be considered as a strategic necessity and a necessary part of doing business in order to survive in the retail banking industry. However, they provide no real competitive advantage to any particular bank as they are not unique, and furthermore, most banks have implemented ATMs with the same basic services (Floyd and Wooldridge, 1990). An empirical study to investigate the impact of ATMs on the local deposit market share of a bank has indeed found little evidence that ATMs deployment offer any competitive advantage in increasing a branch’s share of collection of deposits (Floyd and Wooldridge, 1990, Banker and Kauffman, 1998).

As shown by the preceding example on financial institutions’ ATM services, IT has become a critical ingredient and strategic necessity. Consequently, failure to replicate the same technology threatens financial institutions’ survival (Clemons and Row, 1991, Mahmood and Mann, 2005, Heatley et al., 1995, Ray et al., 2005). As highlighted by Floyd et al. (1990: p. 48) “the costs of [IT] adoption may yield little or no return, but the costs of not adopting are sufficiently high to justify the investment.”

2.3. IT INVESTMENT VALUE

2.3.1. Common Interest on IT Value

With growing level of IT expenditure, as well as the critical role of IT in organisations, the value that IT brings has always been of interest to both practitioners and researchers alike (Chau et al., 2007, Ward et al., 1996, Tanriverdi and Ruefl, 2004, Ravichandran and Lertwongsatien, 2005, Marthandan and Tang, 2010). Based upon these prior studies, and for the purpose of this research, IT value, has been defined as the positive impacts that organisations would obtain from the implementation of their IT systems. IT value has been extensively studied in the IS literature, but seemed to subside at the late 1990s (Chau et al., 2007). However, the interest on IT value research was revived after 2001 following the dot-com bubble burst, where the return of IT investment came into question again (Chau et al., 2007).
Business executives have continued to seek evidence of returns on IT investments, and many are seriously questioning the benefit of their substantial investment in IT (Chang and King, 2005, Mahmood and Mann, 2005). IT is used widely, but it is hard to detect its effects in productivity statistics (Martinsons and Martinsons, 2002). A majority of users are dissatisfied with the value of IT (Peppard et al., 2000), and that IT investments are consistently failing to deliver the anticipated benefits (Ward et al., 2008, Ashurst et al., 2008, Peppard, 2007). Furthermore, a successful delivery of effective IT systems does not necessarily mean that business benefits are attained (Ashurst et al., 2008), and even when benefits are achieved, organisations have struggled to achieve sustainable competitive advantage from their IT investments (Doherty and Terry, 2009).

Some studies have argued that usage of IT alone may not automatically improve profitability, guarantee superior performance or sustainable competitive advantage (e.g. Shin, 2001, Mahmood and Mann, 1993, Lee and Bose, 2002, Alpar and Kim, 1990, Harris and Katz, 1989, Cooper et al., 2000, Peppard and Ward, 2004). In general, IT possesses no inherent value in itself i.e. just having computers on employees’ desks do not create any value to the organisation (Peppard et al., 2000, Peppard et al., 2007). IT provides benefit opportunities (Ward et al., 1996) but the value of IT can only be unlocked or realised by business managers, executives and users (Peppard et al., 2000, Peppard, 2007, Markus, 2004, Peppard and Ward, 2005), as they are the ones who utilise IT on daily basis to attain business goals and objectives. In addition, it is argued that the benefit of IT is acquired through the organisation’s capability to constantly exploit the functionality of IT (Henderson and Venkatraman, 1993), alongside modifications in the way how business activities are done (Ward et al., 1996).

2.3.2. Inconclusiveness of Findings on IT Value

Arising from this widespread interest, IS researchers have attempted to uncover the business value derived from IT investments (e.g. Mahmood and Mann, 2005, Melville et al., 2004, Mahmood and Mann, 1993, Lee and Menon, 2000, Lee and Bose, 2002, Barua et al., 1995). However, demonstrating the consequences of IT utilisation on
organisational performance was found to be challenging (Mahmood and Mann, 2000), and past outcomes have been reported to be conflicting and inconclusive (Lee and Bose, 2002, Barua et al., 1995, Mahmood and Mann, 2005, Tanriverdi and Ruefli, 2004, Ray et al., 2005, Ravichandran and Lertwongsatien, 2005). Some literature have found insignificant or negative impact while others have discovered significant positive effects (Barua et al., 1995).

As highlighted by Barua et al. (1995), studies that found insignificant or negative relationships include Roach (1987), Baily and Chakrabarti (1988), and Loveman (1994). Roach (1987) evaluated the productivity of information and production workers, and concluded that information worker productivity has either deteriorated or has not kept up with the productivity of production worker. Similarly, Baily et al. (1988) concluded that current evidence does not indicate any substantial productivity gain from IT, and had suggested possible explanations such as mismeasurement and organisational inefficiency as the reasons for the unfavourable research outcome. Likewise, Loveman (1994) studied the productivity impact of IT in the manufacturing sector and found no evidence of any significant positive impact from IT.

By contrast, other studies have found some evidence of positive impacts. For example, Lee et al. (2002) have investigated the linkage between IT and organisation’s economic performance by means of aggregated measures of accounting-based and market-based performance. They concluded that various dimensions of IT are significantly and positively linked to a firm’s performance regardless of the various performance measures, and also that IT has a significant effect on aggregated composite measures of accounting-based and market-based performances. In addition, Barua et al. (1995) found that IT inputs have a significant positive effect on the intermediate level output variables for selected strategic business units (SBUs) in the manufacturing sector. Furthermore, a study conducted by Mahmood et al. (2005), which was based on a multi-year analysis of firm-level data, found positive relationships between higher levels of IT investment and selected measures representing organisational performance and productivity.
Chapter 2: Literature Review

IS researchers have tried to provide a number of reasons as to why studies on IT value have resulted in inconclusive findings. One important explanation is said to be attributed to the lack of “unified theoretical framework” that have resulted in diverse and concurrent research paths that are not overlapping one another (Chan, 2000, Melville et al., 2004). Others have attributed this complex problem to unsuitable measurement of outputs, and the delay of several years before IT benefits are realised (Brynjolfsson and Hitt, 1993, Mahmood and Mann, 2005, Brynjolfsson, 1993). In addition, it was also contended that previous research on IT value typically utilised firm-level orientation as the unit of analysis, i.e. using objective financial measures such as firm’s value and return on investment (ROI) (Chau et al., 2007). In this regard, several studies have found that assessing IT value at the firm-level might pose incorrect or misleading results (e.g. Doherty and Terry, 2009, Barua et al., 1995, Ray et al., 2004). One important approach, which is said to provide better representation in the assessment of IT value is through the approach of alternatively conducting similar studies at a more granular process-level outcomes as the unit of analysis, such as from the perspective of individual IS initiative (e.g. Doherty and Terry, 2009, Ray et al., 2005, Bhatt and Grover, 2005). For example, the research conducted by Doherty and Terry (2009) has indeed shown that firm’s ability to attain sustained IT value through individual IS initiatives is positively related to its ability to effectively deploy an appropriate set of IS capabilities.

2.3.3. The Resource-Based View and IT Value

Exploring the relationship between IS capabilities and the attainment of IT value, there is growing evidence, to suggest that an organisation’s superiority in the deployment of capabilities is often considered as a source for competitive advantage (Wade and Hulland, 2004, Day, 1994, Christensen and Overdorf, 2000, Bharadwaj, 2000, Santhanam and Hartono, 2003). Generally, capabilities are regarded as complex combinations of skills and accumulated understanding (Day, 1994), which enable activities that achieve specific objectives, through the usage of organisational resources (Helfat and Peteraf, 2003, Krell et al., 2011). The utilisation of capabilities
by organisations is critical, as it has been suggested that organisations’ survival are being influenced by their IT capabilities (Bharadwaj et al., 1999).

There have been numerous IS studies investigating the role of IS capabilities in facilitating competitive advantage, using the Resource-based View (RBV) as a theoretical lens (e.g. Doherty and Terry, 2009, Wade and Hulland, 2004, Bhatt and Grover, 2005, Bharadwaj, 2000, Santhanam and Hartono, 2003, Mata et al., 1995, Stoel and Muhanna, 2009, Lin, 2007). In this regard, RBV posits that organisations’ resources will allow them to attain competitive advantage, and even further lead to exceptional lasting performance (Wernerfelt, 1984, Wade and Hulland, 2004, Barney, 1991, Grant, 1991, Penrose, 1959). The utilisation of this theoretical perspective is supported by Wade and Hulland (2004), whom has suggested that RBV provides a convincing and robust framework to evaluate the strategic value of IS resources, and therefore would be useful and beneficial in the IS research stream. Correspondingly, Ravichandran and Lertwongsatien (2005) also posit that RBV provides a suitable theoretical lens to analyse how firm’s internal factors can be a source for competitive advantage.

However, due to the diverge frameworks used in this line of study, other researchers such as Doherty and Terry (2009) have argued that one of the key difficulties in using RBV to study the impact of IT on organisational performance, is indeed to select which IT resources and capabilities should be examined. Fortunately, Wade and Hulland (2004) have provided a comprehensive typology of IS resources\(^1\), that can be utilised by researchers. More specifically, their study has suggested eight key IS resources that are organised into three categorisations: inside-out; outside-in; and spanning. Inside-out capabilities are used to react to market requirements and opportunities, and they are initiated from within the firm and tend to be internally focused. By contrast, outside-in capabilities are externally focused, utilised to anticipate market requirements, comprehending competitors and establishing lasting customer relationships. Lastly, spanning capabilities are used to integrate the previous two

\(^1\) The terms resources and capabilities will be considered as synonymous in this research, arising from the recommendations by Doherty and Terry (2009), since they have often been used interchangeably in the past.
categories of capabilities, which involve both internal and external analysis (Wade and Hulland, 2004).

In view of the huge range of conceptual definitions of resources that have been made available in the literature (Galbreath, 2005), the typology of IS resources suggested by Wade and Hulland (2004) - which is primarily based on an earlier work by Day (1994) – have provided a structured and practical insights on the list of IS capabilities that would be useful in the effort to attain value for the organisation. Therefore, based upon the above discussions, adopting the RBV framework as the theoretical lens, could be one of the best alternatives for IS researchers to effectively gain insights into the value of organisational IT investments.

2.4. IT AND REGULATORY COMPLIANCE

2.4.1. Significance of Regulatory Compliance

Besides IT’s pervasiveness and the longstanding interest in ascertaining the value of IT investments, an equally important factor that is also influencing IT deployment and operations, in the financial industry, is the need to comply with various regulatory requirements. In this context, regulatory requirements, can be defined as a form of obligatory requests from the regulatory authority that typically dictate and restrict the general behaviour of financial institutions, and often pertaining to a specific area of concern, such as on anti-money laundering and counter financing of terrorism (AML/CFT).

Several researchers have acknowledged that the financial industry is one of the most heavily regulated industries (Fisher and Harindranath, 2004, Weidenmier and Ramamoorti, 2006, Garcia, 2004), due to its propensity to attract the interest of criminals (Fisher and Harindranath, 2004, Kay, 1999). The regulatory authority that is imposing regulatory requirements upon the financial industry is typically focusing on promoting financial stability and integrity, and high standards of conduct (Kay, 1999, Hüpkes and Zibung, 2008), as well as, protecting depositors and investors (Fisher and Harindranath, 2004, Hüpkes and Zibung, 2008, Alam, 2012). For regulated entities,
not abiding by these regulatory requirements will likely expose them to potentially adverse consequences, as regulatory breaches can often lead to hefty fines or lawsuits, damage to reputation or even loss of license to conduct business (Fisher and Harindranath, 2004, Weidenmier and Ramamoorti, 2006, Cravens et al., 2003, Garcia, 2004, Adams, 2012). As an example, in a recent case involving the HSBC Bank, the institution had been heftily fined USD1.9 billion by the U.S. authorities arising from its failed AML/CFT controls. In this regard, the bank had been alleged to have allowed proceeds from drugs and financial transactions from countries being sanctioned to enter the U.S. financial system (e.g. Berthelsen et al., 2012, BBC News, 2012).

2.4.2. Common Standpoint on Regulatory Compliance

Existing literature relating to regulatory compliance, which refers to organisational activities that are induced or stimulated by requirements issued by the regulatory authority (e.g. Elliehausen, 1998, Gable, 2005), has typically painted a negative picture with regard to its impact on the organisations being regulated. Some researchers have argued that regulatory compliance is costly and absorbs significant resources (e.g. Walter and Rolf, 2005, van Oosterhout et al., 2006, Elliehausen, 1998, Garneau and Shahid, 2009, Gable, 2005, Pakravan, 2011), as well as creating lower efficiency (e.g. Barth et al., 2004, Barth et al., 2001, Guasch and Hahn, 1999, Hüpkes and Zibung, 2008). It is estimated that up to 15 percent of any organisations’ IT budgets is spent upon complying with regulatory requirements (Gartner Corporation, 2006a, Krell and Matook, 2009).

This form of external influence, which is naturally beyond the control of organisations or the industries, in which they operate, will dramatically affect organisations’ IT infrastructure (Gregor et al., 2006). Regulatory requirements impacting upon IT are said to be time consuming to implement due to the typically large and complex legacy systems that are organised in different silos, and managed by different vendors (van Oosterhout et al., 2006). The overall cost of implementing new IT solution due to regulatory requirements is also considered as burdening due to the additional hardware and software needed, the associated user training required, and
interruptions to existing processes, etc. (Krell et al., 2011, Hitt et al., 2002, Jiang et al., 2000). In addition, it is likewise argued that these requirements influence the firm’s performance by imposing barriers to entry (thus raising prices and profits), anticompetitive practices, limits profit-making potential and may even lead to the distortion of the level playing field between local and foreign players (Peltzman, 1973, Bharadwaj et al., 1999, Kahn, 1988, Jarrell, 1984, Helmuth, 1990, Paul et al., 2008).

The cost of regulation imposed by government has developed into a political issue (Elliehausen, 1998) over concerns about the excessive cost and administrative burden imposed by complying with regulatory requirements (Raghavan, 2007). Many politicians are criticising the burden imposed by regulation, but regulatory requirements are hardly ever revoked, and new laws continue to be endorsed, imposing greater regulation (Elliehausen, 1998). As existing firms have already endured the fixed cost of implementing regulation, they have no motivation to lobby for a reduction of regulatory requirements for new entrants (Franks et al., 1998), which can also partly be used to explain why regulations are seldom revoked. Significant events such as the global subprime crisis have even led to the discussion on the possibility of more stringent regulatory requirements to be deployed in the financial industry (Paul et al., 2008, Hüpkes and Zibung, 2008).

2.4.3. Role of IT in Regulatory Compliance

An increasing number of regulations (such as Sarbanes-Oxley Act 2002 (SOX); Basel II; Gramm-Leach-Bliley Act of 1999; USA PATRIOT Act; HIPAA; and pertaining to AML/CFT) are regarded to be impacting organisations’ IT infrastructures and processes in order to ensure compliance (Luthy and Forcht, 2006, Volonino et al., 2004, Adams, 2012). However, it is important to note that since regulatory requirements tend to be more primarily focused upon outcomes, little insight is usually given on how compliance is to be achieved, including whether the utilisation of IT would specifically be required to effectively facilitate compliance (Luthy and Forcht, 2006, Lurie, 2004, Gable, 2005). Nevertheless, due to the intricacy and timeliness nature of regulatory reporting, they can only be best achieved through heavy reliance on IT systems (Volonino et al., 2004,

The complexity and the demands of regulatory reporting can be seen in the case of requirements from SOX, which specifically holds senior management of public companies (i.e. CEOs and CFOs) personally liable for the effectiveness of internal controls established for reporting and disclosure of financial statements, making them accountable to validate detailed financial statements, as well as how they are prepared (Damianides, 2006, Lurie, 2004). In addition, in the effort to meet part of Basel II requirements, financial institutions will need to perform massive system changes in order to leverage their IT systems to capture and categorise data needed for large scale credit risk modelling to profile and monitor credit risk exposure (Blount, 2004, Swartz, 2005). Furthermore, similar to SOX, Basel II also requires senior management to personally attest the effectiveness of internal controls with the financial reporting (Waring, 2006).

As seen in the previous sections, IT is extensively employed in financial institutions and is often regarded as a strategic necessity where failure to duplicate similar technology threatens their very survival. Therefore, due to the pervasiveness of IT in financial institutions and its position, at the centre of all business and operational activities (Damianides, 2006, Luthy and Forcht, 2006), IT has also become a critical central component that facilitates any organisations’ ability to cost-effectively comply with regulations (Damianides, 2006, Lurie, 2004, Volonino et al., 2004). The use of IT for compliance is impacting on areas such as data collection and processing, audit trail, database management, security, fraud, systems failure, and service delivery (Luthy and Forcht, 2006). Interestingly, with regard to the earlier example on regulatory penalties being imposed on HSBC Bank [see Section 2.4.1], increased spending on its AML/CFT IT systems had been cited as one of the solutions to ensure similar incidents will not occur in the future (e.g. Mollenkamp and Wolf, 2012, BBC News, 2012).

Moreover, as regulatory requirements may be imposed on an organisation as a whole, which includes any of its foreign operations operating worldwide (Luthy and Forcht, 2006), compliance could not possibly be effectively achieved without highly leveraging
IT infrastructure and capabilities. With these mandatory requirements imposed by regulations, IS professionals are also exposed to increased challenges and raised expectations, as well as having resulted in the management of information as both a business importance and a legal responsibility to meet regulatory requirements (Volonino, 2007, Damianides, 2006). For example, according to Volonino et al. (2004), regulatory demands on IT from SOX are like those of Y2K, but in this case, are happening four times in a year due to the quarterly filing to the US Securities and Exchange Commission (SEC).

2.4.4. Alternative Approach to Regulatory Compliance

As seen in the earlier discussion, industry’s view of the implementation of regulatory requirements has largely been unenthusiastic since they are typically regarded as costly and resource demanding. While this situation is totally understandable, there are nevertheless differing discussions in the literature that have drawn interest to a contrasting perspective, i.e. namely leveraging regulatory compliance activities, to directly benefit the organisation’s business in one form or another.

However, it may be worth noting at this juncture that the nature of benefits mentioned through this particular line of thinking are not mainly reflecting the regulatory authority’s ultimate objectives for introducing the requirements in the first place. If viewed specifically from the regulators’ standpoint, the value enhancing intention can, in effect, be regarded as principally from the contexts of improving and enhancing organisation’s risk management practices; overall control environment; and investor’s trust and confidence (e.g. Hall, 2006, Damianides, 2006, Waring, 2006, Fischer, 2008). On the other hand, this alternative and distinct line of thinking can be regarded as a departure from the regulatory authority’s ultimate intention, and it is primarily focusing on two broad perspectives i.e. increasing the efficiency and effectiveness of overall regulatory compliance efforts; as well as the possibility of utilising these activities as a catalyst to directly benefit the organisation’s business.

It is important to note that for the purpose of this study, the term ‘benefits’ will be used as a proxy to refer to IT value. This is done in order to clearly distinguish the two
aspects of IT value that are associated with compliance led IT investments. The
definition for these two types of benefits, i.e. compliance benefits; and supplementary
benefits, will be explained in detail in Chapter 3 [see Section 3.3].

a) Enhancing Efficiency and Effectiveness of Compliance Activities

Exploring the first perspective of potential benefits, this viewpoint is seen to be rooted
on the understanding that regulatory requirements are typically unavoidable and thus
need to be adhered to. Therefore, the possible benefits suggested by this viewpoint
are in the form of increasing organisations’ compliance efficiencies, and effectiveness
in achieving the intended regulatory objectives and outcomes, such as through
eliminating redundancy of efforts and using common approaches. Literature in this
regard has highlighted that dealing with each regulation individually or treating them
as an isolated event just for the sake of complying will be ineffective and costly as they
are too many, too complex and will increase over time (Lurie, 2004, Mayer, 2003,
Schlarman, 2007).

Therefore, this body of literature has called for the minimisation of compliance costs
through identifying similar IT changes required, such as by SOX and Basel II, and
performing them simultaneously or concurrently (e.g. Mayer, 2003). A single set of
controls can be used to comply with multiple regulations due to the similarity in the
way data are arranged and the common requirement of regulations to maintain data
integrity and security (Wagner and Dittmar, 2006). Indeed, SOX and Basel II do
contain many similarities, such as: both cover the breadth and depth of the institution;
stress the timeliness of critical information; emphasise the need for controlled,
reliable and accurate data capture and reporting; and the criticality of information
management (Mayer, 2003). Similarly, Gable (2005) has also suggested that
organisations take a broader approach by establishing compliance programs that
include common methodologies, structures and templates for meeting existing and
expected compliance requirements. In addition, compliance approaches may be
premised on risk assessments and mitigation efforts that acknowledge responses to
multiple simultaneous requirements and provide a way to assign priorities (Gable, 2005).

b) Extending Beyond Regulatory Purposes

In relation to the second perspective of potential benefits, another body of literature has called for viewing compliance activities beyond mere regulatory purposes. This goal can be achieved by taking the opportunity to incorporate extended activities, additional considerations or optional changes that may directly benefit the organisation’s business. This type of potential benefits can partly be attributed to the earlier understanding on regulatory requirements, which typically highlight the expected goals and outcomes, without normally explaining the means (Luthy and Forcht, 2006, Lurie, 2004, Gable, 2005). Therefore, it is sensible to view the possibility of organisations taking the opportunity to incorporate additional goals and objectives to be achieved within the compliance implementation, as discussed below.

Garcia (2004) has suggested that organisations that are forward-thinking should combine tactical business requirements with strategic performance opportunities, and view compliance as an opportunity not only to mitigate risk and increase efficiency, but also to transform business processes and improve business performance. Using this approach, it is proposed that firms will not only meet regulatory requirements but also seize the opportunity to implement concurrent IT enhancements that support valid business goals. For example, compliance systems that detect suspicious activities (such as in the case of AML/CFT efforts) can be used to understand the customer better and to achieve improved cross-selling and enhance customer retention. Furthermore, it is said that IT investments due to compliance should be in line with the greater good of the organisation and should pay for itself in the long term (Garcia, 2004).

In addition, Volonino et al. (2004) have highlighted that if organisations view regulation as an opportunity to enhance operations, they will be able to gain prolonged strategic value from business improvements and competitive advantage. In order to gain maximum return on investment in compliance and enable IT to
contribute to the long term growth, organisations should approach compliance holistically i.e. by among others involving redesigning business processes; enhancing information quality and risk management; and codifying organisational knowledge within their compliance efforts (Volonino et al., 2004). Furthermore, Damianides (2006) had suggested that, in the case of SOX requirements, some organisations have shifted their focus from compliance as a necessary evil to compliance as a competitive advantage. These organisations are said to have ceased complaining about SOX and have altered their compliance efforts to more effectively control their operations, whilst also reducing compliance costs (Wagner and Dittmar, 2006). Furthermore, it was highlighted that some executives that recognised SOX’s advantages at the onset have indeed figured out how to utilise the new regulations to realise organisational improvement plans (Wagner and Dittmar, 2006).

c) Insights from Existing Empirical Studies

It is important to note however, that all the aforementioned literature which has explicitly promoted the idea of regulatory compliance for business benefits, can be classified as conceptual or non-empirical studies. Non-empirical literature, in this context, is predominantly based on ‘ideas, frameworks and speculation’ as compared to empirical literature that rely on systematic observation and data (Alavi and Carlson, 1992, Van Horn, 1973, Chen and Hirschheim, 2004). Some researchers (e.g. Melville et al., 2004) have drawn attention to the fact that very little is known about industry characteristics (i.e. includes regulatory requirements) and their relationships with IT business value. These researchers go on to suggest that this is an area worthy of further research. Unfortunately, few studies seem to have explicitly attempted any empirical investigation of regulatory implementation, in an organisational context.

Nevertheless, regulation has indeed been mentioned in several IS studies, though not from the explicit perspective suggested by this research. For example, in a study conducted by Bharadwaj et al. (1999), regulation was used as a dummy variable to classify whether firms included in the analysis, operated in a regulated industry or not. Another study conducted by Hu et al. (2007) attempted to explore how SOX regulation
and internal influences had affected the organisation’s information systems security implementations. However, it is important to note that the results of the study by Bharadwaj et al. (1999) did not explicitly explore the value from compliance, as the result has only shown that regulated industries are negatively viewed by the marketplace. In relation to the study conducted by Hu et al. (2007), it was found that SOX’s compliance was used as one of the rationale for initiating modifications to organisational processes. In this specific context, the Chief Operating Officer (COO) of the case study organisation had been seen to use the external pressure from SOX “for all the right reasons” and aiming to be “a better business” by “hiding behind it” (Hu et al., 2007: p. 162). Nonetheless, it is important to note that the study was not specifically intended to explore the possible value of regulatory IT implementations.

In another study of a similar nature, there was an attempt to explore the effectiveness of formal planning methods, which addressed both mandatory IS investments and optional organisational requirements, for selected low-cost firms in Australia. In this study, conducted by Krell and Matook (2009), the mandatory IS investments imposed by government regulations are regarded to be over and above the expected IS expenditure, relating to normal business needs. The researchers argue that by utilising formal planning methods (i.e. business cases; internal contractual arrangements; and post-implementation reviews), low-cost firms would be able to combine mandatory and optional investments that would facilitate the attainment of competitive advantage.

Results of the study indicated that only two out of three investigated formal planning methods are positively related to competitive advantage. In this regard, the researchers has suggested that most low-cost firms do not use formal planning methods when mandatory IS investments are imposed upon them, mainly due to an attempt to reduce associated compliance expenditures.

It may worth noting at this point that Krell and Matook’s (2009) work have no similarity to the specific context of the study that will be presented in this thesis. Yet, it is motivating to appreciate that their effort has indeed highlighted the research opportunity of empirically exploring the possibility of leveraging regulatory IT
implementations to directly benefit business. Therefore, the work of these researchers has somehow strengthened the case for this thesis, as well as provided extra comfort on the significance of a study of this nature.

From a slightly different perspective, it may also worth noting that several studies have attempted to understand the cost-benefit impact of regulation on firms. In an effort to gauge the economic impact of regulation, the US government had started using the cost-benefit analysis (CBA) approach in 1997 (Hahn, 1998) and followed by a few other countries including the United Kingdom (Alfon and Andrews, 1999). This has led to several discussions on the CBA approach in the literature (e.g. Hahn, 1998, Guasch and Hahn, 1999, Alfon and Andrews, 1999). Nevertheless, leaving aside the discussion on evaluation of regulatory cost, it is worth noting that the assessment of benefits in the CBA approach has been predominantly assessed from the perspective of the economic benefits, such as the reduction in the likelihood of financial system failure and the increase in consumer’s surplus (Alfon and Andrews, 1999). Therefore, these studies were not done from the perspective of IT value and could not be considered as the type of research that can be classified under the IS domain.

Moving the discussion to view mandatory investments from the perspective of organisational IT systems evaluation, several researchers have acknowledged the potential influence of regulatory related requirements in the evaluation of IT systems in organisations. Howcroft (2004) had mentioned that different regulative processes is one of the factors that may influence the design and use of IT systems, and Farbey et al. (1999) meanwhile acknowledged that external stakeholders (such as government via regulatory requirements) can indeed play a significant and critical role in many IT investments. In addition, Serafeimidis et al. (1996) had also pointed out that IT system evaluations may comprise of external factors that are beyond the organisation’s control but needed to be responded and accommodated accordingly.

However, evidence from literature seemed to suggest that organisations are lacking in actively consider regulatory requirements in their IT systems evaluation routine. Most cases within the literature, organisational IT systems evaluation is predominantly discussed from the feasibility perspectives i.e. concerning proper appraisal of capital IT
investments via pre-project considerations and justifications approaches to identify and evaluate potential cost and benefits, as to determine whether the investment brings value, and whether it should go ahead or otherwise (e.g. Ballantine et al., 1996, Farbey et al., 1992, Ward et al., 1996, Farbey et al., 1999, Apostolopoulos and Pramataris, 1997, Arnovick and Gee, 1978, Irani and Love, 2001). As it is, evaluation of IT systems is said to be a complex activity due to the difficulty in determining the value of information (Arribas and Sánchez Inchusta, 1999, Serafeimidis and Smithson, 1996). Also, significant levels of intangible factors are used before decision on IT investments are made, making them hard to measure and quantify (Tingling and Parent, 2004).

Therefore, there is lack of evidence from the existing literature, regarding IT system evaluation, that has provided insights regarding compliance implementations, i.e. whether they have actively considered non-mandatory or optional elements in their compliance approach or action plan. On the contrary, existing knowledge of IT evaluation practices for business IT systems are seen to be primarily driven by the sole aim to achieve value from business IT investments. In a nutshell, the literature on IT system evaluation has suggested that activities concerning business and compliance implementations to be mutually exclusive, i.e. driven by contrasting factors.

2.5. CONCLUDING REMARKS

This chapter has attempted to provide a detailed overview of the existing literature relating to value of IT investments and regulatory compliance. The review of these extant bodies of knowledge will set the scene for the discovery of important research gaps within the study. In this regard, the gaps identified will in general, form the theoretical foundation for the study, offer the justifications for the research, as well as justifying the knowledge it is trying to enhance. The chapter that follows will elaborate in detail the identified research gaps, the research objectives, as well as provide a presentation on the conceptual research framework that will be utilised to structurally and empirically explore the specific area of interest.
Chapter 3
Research Objectives and Framework

3.1. INTRODUCTION
Having reviewed the literature regarding value of IT investments and regulatory compliance, this chapter will continue with the discussion by presenting the associated research gaps that have been uncovered, and therefore showcasing the specific areas that may indeed worth further investigation. In addition, the chapter will also outline the identified research objectives and the conceptual research framework that are deemed suitable to effectively explore the identified areas of interest. Both the research objectives and the conceptual research framework will attempt to structurally address the identified research gaps, and hence, it is envisaged that they will be able to aid in attaining the knowledge that the research is seeking to contribute.

This chapter is generally divided into three broad sections, with the initial discussions of the identified research gaps arising from the review of the literature. This is then followed by the second section elaborating the rationale for the identified research objectives. Subsequently, the last broad section presents the discussions on the conceptual research framework that are anticipated to allow the research gaps to be effectively examined. All the above are brought to close by the concluding remarks, which provides the summary and conclusion to the chapter.

3.2. CRITIQUE OF EXISTING LITERATURE
Arising from the review of the literature [see Chapter 2] within the two broad domains of knowledge (i.e. value of IT investments and regulatory compliance), it can therefore be concluded that there are indeed a number of research gaps that warrant empirical
exploration. The research gaps identified and described in the following paragraphs will form the foundation for conducting this study, as well as outlining the specific area of knowledge that it will seek to contribute.

Overall, it appears that there is lack of empirical research that has attempted to explore the possible value from IT investments, specifically relating to banking institutions’ regulatory implementations. As discussed in the earlier chapter, banking institutions’ IT infrastructures and processes are extensively impacted by regulatory requirements (e.g. Luthy and Forcht, 2006, Volonino et al., 2004), as well as being widely utilised for meeting regulatory expectations (e.g. Volonino et al., 2004, Lurie, 2004, Damianides, 2006). However, existing literature has provided little evidence of how regulatory IT implementations could provide value to banking institutions through basic compliance activities. Moreover, there have been no previous studies that have explicitly presented examples of business value being generated from activities beyond mere regulatory compliance.

In this regard, a study enhancing our understanding in this respect would indeed be an interesting area that is worth further exploration. The importance of a study of this nature can further be attributed to the anticipation that more, as well as stricter regulations are likely be imposed in the future.

It is important to distinguish between these research gaps. In relation to possible value arising from basic compliance activities, it is envisaged that this objective can be accomplished through, for example, minimising the associated compliance cost (i.e. by reducing the redundancy of efforts through identifying similarities in requirements and performing required IT changes simultaneously) (Mayer, 2003). On the other hand, with regard to potential value that is directly benefiting banking business from activities beyond basic regulatory compliance, this goal can be attained by, for instance, through conducting a dual purpose compliance spending (Garcia, 2004).

Even though Krell and Matook (2009) had explicitly explored the incorporation of optional requirements within mandatory IT investments, in order to achieve

---

2 As mentioned in Chapter 2, one way of achieving this type of benefit is by incorporating optional investments, over and above mandatory IT investments, in order to benefit organisation’s business.
competitive advantage, the low-cost firms used in their study are of contrasting nature to banking institutions. In this regard, banking institutions can, in effect, be regarded as higher-cost institutions, and thus may likely be subjected to a different form of mandatory deliverables and expectations arising from contrasting regulatory backgrounds. In addition, the rationale for selecting banking institutions as the entities to be studied can also be attributed to the earlier discussions acknowledging the financial industry as being one of the heavily regulated industries due to its potential adverse systemic impact to the economy (Fisher and Harindranath, 2004, Kay, 1999). This unique situation is over and above to the appreciation that these institutions are also critically leveraging on IT to survive and excel (e.g. Berger, 2003, De Haes and Van Grembergen, 2008, Ray et al., 2005, Vitale, 1986, Lee and Bose, 2002), as well as importantly, to facilitate cost-effective compliance (e.g. Swartz, 2005, Damianides, 2006, Volonino et al., 2004, Blount, 2004).

Furthermore, the review of existing literature has also revealed that insights into the role of IS capabilities to efficiently and effectively satisfy regulatory requirements and accomplish the expected deliverables (and thus the associated benefits) has yet to be sufficiently investigated. In addition, the function of these capabilities in facilitating the likelihood of direct benefits to banking business has still to be fully understood. Therefore, this third research gap that has been identified arises from the lack of understanding on how these associated IS capabilities are potentially facilitating the two variations of benefits that are of interest in this study.

Lastly, the fourth research gap can be attributed to the similarly lacking existing studies that has explicitly explored the impact on the banking institution’s competitive positioning, arising from effective deployment of IS capabilities to meet regulatory requirements. In this regard, the impact of banking institution’s competitive positioning may emerge from the attainment of both variations of benefits mentioned in the preceding discussions. In addition, it may be worth reemphasising that exploring the role of IS capabilities from this specific perspective is indeed appealing. This view can be attributed to the growing evidence that suggests the superiority for the deployment of capabilities is often considered as a source for competitive advantage for organisations (e.g. Wade and Hulland, 2004, Santhanam and Hartono,
2003). It may be worth reiterating that the general approach undertaken by this research will indeed be in contrast to Krell & Matook’s (2009) work. In this regard, the study will not primarily be confined to the utilisation of formal planning approaches in the attempt to assess the achievement of competitive advantage arising from regulatory compliance activities.

### 3.3. RESEARCH OBJECTIVES

Moving the discussions to the identified research objectives, in general, there are four research objectives that have been identified to effectively address the research gaps in the previous section. However, before the discussion can proceed to discuss on the above, it is worth noting at this juncture that there is another key underlying principle (besides the literature) that has guide the formulation of these research objectives. This approach is adopted particularly to ensure that they will correspond with the overall motive of this research.

In this regard, it is important to note that the identified research objectives will not be aiming to gain insights from the perspective of expected deliverables, achieved through the banking institution’s activities to meet regulatory requirements. In this regard, deliverables have been defined as *all forms of outcomes that are expected to be achieved by organisations arising from the adherence to regulatory requirements.* Instead, these research objectives are designed to explore from the context of possible benefits that may be experienced through these regulatory activities. **Benefits,** in this situation, have been defined as *the favourable resulting condition or circumstance, arising from the accomplishment of the expected deliverables.* In other words, only by attaining these expected deliverables will the situation allows for benefits to possibly be experienced by organisations.

The rationale to follow this approach can further be explained from the appreciation that regulatory deliverables, can be considered to be largely embedded within the requirements, imposed by the regulatory authority. As highlighted earlier during the review of the literature, it has indeed been acknowledged that the nature of regulatory requirements would typically highlight what needs to be achieved (and
therefore defines the expectations on the various deliverables required. This is typically done without providing detailed explanation on how to achieve them (Luthy and Forcht, 2006; Lurie, 2004; Gable, 2005).

Additionally, various deliverables achieved, by meeting regulatory requirements, may effectively present similar or overlapping benefits to the organisation. In other words, several expected regulatory deliverables may, in effect, produce a single benefit. Therefore, in line with the overall intention to gain insights into possible value of regulatory IT implementations, and given that the expected deliverables can largely be determined from the regulatory requirements, it would instead be more interesting for the research to explore from the viewpoint of potential benefits.

Going forward, it may be critical to appreciate as well that there are two types of benefits that will be explicitly explored within this research. For the purpose of this study, the first type of benefit, known as compliance benefits, have been defined as expected or anticipated outcomes, arising from organisation’s efforts to simply meet regulatory requirements. Compliance benefits are therefore accomplished through implementing the fundamental activities required and thus achieving the expected regulatory deliverables. Importantly, they are also achieved in order to avoid any potential penalties that may be imposed due to lack of compliance. In contrast, the second type of benefit, known as supplementary benefits, have been defined as those benefits that are achieved over and above to the ones that are usually expected and anticipated, and therefore seen to directly benefitting banking business. These benefits are achieved through the ability to broaden the fundamental efforts of regulatory compliance, i.e. arising from the activities beyond the act of complying with regulatory requirements.

The elaboration on the four research objectives that have been identified from the perspective of the aforementioned attainable benefits is provided in the following discussions. The research objectives were developed after recognising the importance of them being clearly focused, as well as in ensuring that they are related with one another and further to “form a coherent set of issues” (Bryman, 2008: p. 73). For ease of comprehension, a table outlining the identified research gaps, in contrast to their
relevant research objectives (as well as the associated chapters where they will be explained in detail), is presented in Table 3-1 below:

Table 3-1: Identified Gaps in Comparison to Research Objectives

<table>
<thead>
<tr>
<th>Gap in Literature</th>
<th>Research Objective</th>
<th>Chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value from basic compliance activities</td>
<td>RO1a: To understand the overall approaches and mechanisms by which banking institutions translate the regulators’ requirements into functional specifications for their compliance system;</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>RO1b: To understand and appreciate instances of compliance benefits arising from banking institutions meeting the regulatory requirements.</td>
<td>6</td>
</tr>
<tr>
<td>Value from broader compliance activities</td>
<td>RO2a: To understand the approaches and mechanisms by which banking institutions take into account other influences, when responding to regulators’ requirements;</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>RO2b: To understand and appreciate instances of supplementary benefits that directly benefit banking business, arising from banking institutions decision to leverage compliance activities.</td>
<td>7</td>
</tr>
<tr>
<td>Role of IS capabilities in facilitating value</td>
<td>RO3: To explore and understand the banking institutions’ portfolio of IS capabilities that are being utilised to facilitate both compliance and supplementary benefits.</td>
<td>8</td>
</tr>
<tr>
<td>Impact on competitive positioning</td>
<td>RO4: To investigate how through the utilisation of capabilities in realising compliance benefits and supplementary benefits, a financial institution might improve its competitive positioning.</td>
<td>8</td>
</tr>
</tbody>
</table>

3.3.1. Value from Basic Compliance Activities

RO1a: To understand the overall approaches and mechanisms by which banking institutions translate the regulators’ requirements into functional specifications for their compliance system;

RO1b: To understand and appreciate instances of compliance benefits arising from banking institutions meeting the regulatory requirements.

The first research objective comprises of two goals that aim to ascertain the possible value that may arise from basic compliance activities. The first part of the research objective aims to appreciate banking institutions’ approaches and mechanisms to translate regulatory requirements into functional specifications, and thus meeting the
expected deliverables and avoiding regulatory penalties. The second part of the research objective, meanwhile, aims to appreciate the accomplishment of expected compliance benefits arising from this type of activity. Performing basic regulatory activities, in this regard, will only aiming to accomplish the intended regulatory deliverables, without exploring the potential of implementing any other activities, considerations or changes that could directly be of advantage to the business of banking institutions.

As suggested by the literature, banking institutions should ensure the efficiency and effectiveness of basic compliance activities by minimising the cost of compliance via reducing redundancies, such as through; addressing similar required IT changes and performing them simultaneously (e.g. Mayer, 2003, Wagner and Dittmar, 2006); or using common methodologies, structures and templates (e.g. Gable, 2005); etc. In relation to this, the research objective will therefore covers the possibility of banking institutions addressing than one regulation at the same time. In addition, it will also deal with the possibility of them leveraging existing compliance processes to address any new requirements that may have some similarities in the needed implementation or the anticipated regulatory outputs.

3.3.2. Value from Broader Compliance Activities

RO2a: To understand the approaches and mechanisms by which banking institutions take into account other influences, when responding to regulators’ requirements;

RO2b: To understand and appreciate instances of supplementary benefits that directly benefit banking business, arising from banking institutions decision to leverage compliance activities.

The second research objective also comprises of two goals. The first part of this research objective is to explore any instances where banking institutions have indeed taken the effort to implement a broader approach to compliance activities that are beyond mere regulatory purposes. Meanwhile, the second part of this research
Chapter 3: Research Objectives and Framework

Objective was to appreciate whether banking institutions are experiencing business benefits from compliance activities. In this regard, it is envisaged that leveraging regulatory compliance offers banking institutions the opportunity to possibly achieve positive IT business value, or in relation to this research, being regarded as the accomplishment of supplementary benefits.

In relation to the broader approach to regulatory compliance, it may indeed be realised by incorporating extended activities, additional considerations or optional changes that could be of direct benefit to the banking institution’s business (i.e. such as; improving business performances; bringing valuable business efficiencies; or supporting valid business goals). In addition, as highlighted by the literature, supplementary benefits may be realised by initiating measures such as; combining tactical business requirements with strategic performance opportunities; dual purpose of compliance spending by taking the opportunity to incorporate additional or optional activities in addition to mandatory investments (Garcia, 2004). Alternatively, they can also be obtained by implementing holistic compliance processes through redesigning of business processes (Volonino et al., 2004); etc.

Therefore, this research objective addresses the deliberate incorporation of supplementary business related activities that are aimed at directly benefiting banking business, and achieving added outcomes that are over and above the expected deliverables due to regulatory implementations. Furthermore, this specific research goal is to be achieved without strictly exploring from the potential effectiveness of deploying any formal planning methods, which will be in contrast to Krell and Matook’s (2009) work on low-cost firms in Australia. Therefore, it is envisaged that banking institutions will have the opportunity to improve their business by directly leveraging compliance activities that are needed to be deployed, without specifically limiting the opportunity to achieve this aim through any specific method of implementations.
3.3.3. Role of IS Capabilities in Facilitating Value

RO3: To explore and understand the banking institutions’ portfolio of IS capabilities that are being utilised to facilitate both compliance and supplementary benefits.

The third research objective aim to explore and understand the list of IS capabilities that have assisted banking institutions to attain expected compliance benefits. In addition, it is also intended to appreciate the list of IS capabilities that have possibility facilitated the achievement of supplementary benefits.

The above research objective to explore the role of IS capabilities in facilitating compliance, as well as supplementary benefits is largely rooted on the increasing evidence suggesting the superiority of capabilities deployment that is frequently regarded as a source for competitive advantage (e.g. Wade and Hulland, 2004, Santhanam and Hartono, 2003). Hence, it is envisaged that in the effort to attain compliance benefits, as well as supplementary benefits, banking institutions will need to utilise their IS capabilities to ensure the attainment of possible value from regulatory IT implementations. In this regard, the Resource-based View (RBV) theoretical perspective will be used to explore the role of IS capabilities in achieving these possibilities. The application of RBV in this research, principally based on the work of Wade and Hulland (2004), will be elaborated in detail in the Research Framework section of this chapter.

3.3.4. Impact on Competitive Positioning

RO4: To investigate how through the utilisation of capabilities in realising compliance benefits and supplementary benefits, a financial institution might improve its competitive positioning.

The final research objective aims to gain insights into whether the attainment of expected compliance benefits through by the utilisation of associated capabilities, have indeed positively influenced banking institution’s competitive positioning. Similarly, it is also aimed to explore whether the attainment of supplementary benefits
through the usage of relevant capabilities have likewise provided a similar influence as well.

It is sensible to conceive that basic regulatory compliance activities may have less influence on banking institution’s competitive positioning. This situation will be in contrast to the broader approach which has deliberately incorporated additional outcomes and intentions which in effect, are aimed to directly benefit banking business. Nevertheless, it may be worth noting that banking institution’s competitive positioning could still be influenced by these fundamental compliance activities, arising from the distinctiveness of each institution. In addition, it may also be attributed to the institution’s unique ability to reduce compliance cost by successfully deploying more efficient and effective compliance activities, which may not be similarly achievable by other organisations within the industry.

Therefore, having presented the above four research objectives that have been identified to specifically address the identified research gaps, the section that follows will explain in detailed the conceptual research framework that have been designed for this study. It is envisaged that the research framework will be able to effectively explore the identified gaps by putting these research objectives into perspective, in the effort to meet the overall intention of this research and achieve the knowledge that it is seeking to contribute.

3.4. CONCEPTUAL RESEARCH FRAMEWORK

3.4.1. Potential Relationships

As mentioned earlier, the conceptual research framework will provide detailed explanation of how the research objectives identified in the preceding section will be mapped to the overall context of the research. Although this research is primarily exploratory in nature, the discussion on the research framework will nevertheless illustrate the plausible direction of causality for this study. This is done in order to assist in the understanding on the potential relationships that may exist, as well as to aid in setting the focus and boundary (Miles and Huberman, 1994) of the study. This
approach is supported by Marshall and Rossman (1995: p. 33) who highlight that exploratory research aims to “identify plausible relationships shaping the phenomenon”, and assesses at how relevant forces “interact to result in the phenomenon”. In addition, Miles and Huberman (1994: p. 17) have also highlighted that “any researcher, no matter how unstructured or inductive, comes to fieldwork with some orienting ideas.” Therefore, taking cue from these statements, the conceptual research framework that outlines these potential relationships is portrayed in Figure 3-1 below:

![Figure 3-1: The Conceptual Research Framework](image)

Viewing Figure 3.1 from the left hand side, the two types of influence that are impacting banking institutions’ ability to attain compliance benefits, as well as supplementary benefits has been regarded as mandatory influence and optional motivation. Mandatory influence in this regard is considered to be driven by regulatory requirements, while optional motivation is seen to be encouraged by other influences such as discretionary business requirements, over and above to the mandatory requirements (e.g. Krell and Matook, 2009, Hu et al., 2007). The combination of these two influences (represented by the rectangular dotted lines) is regarded as the key motivating factors that are affecting banking institution’s ability to experience compliance benefits, as well as any instances of supplementary benefits.
In addition, the overlapping rectangles (which provide mandatory influence) indicate the possibility of more than one type of regulatory requirements are affecting banking institutions at a similar time interval. They are therefore suggesting that banking institutions would have the opportunity to efficiently and effectively minimise the cost of compliance by reducing redundancies, such as by addressing similar requirements simultaneously (e.g. Mayer, 2003, Wagner and Dittmar, 2006). Furthermore, they are also aimed to indicate the possibility of banking institutions leveraging existing compliance establishments to address any emerging requirements that may have similarities in the required regulatory implementations or the anticipated regulatory outputs, for example, by way of using common methodologies, structures and templates (e.g. Gable, 2005).

With regard to the discussion on capabilities, the two arrows indicate that a same set of capabilities might be needed to effectively accomplish both compliance benefits and supplementary benefits. However, these relationships do not in any way ignore the possibilities of some discrepancies between the needed capabilities that may exist for the two categories of benefits. In addition, they also do not disregard the prospect of any other additional capabilities (beyond the ones that will be suggested in this research) that may influence the attainment of compliance benefits, or the supplementary benefits. Furthermore, with the aim of gaining deeper insights into the type of capabilities that might be useful to explain the attainment of both benefits, the taxonomy of IS capabilities suggested by Wade and Hulland (2004), will initially be employed as the basis for the assessment. Detailed explanation on the application of the suggested taxonomy of IS capabilities in this research will be explored in the subsequent section.

Moving forward to the next plausible relationships, it is envisaged that banking institutions’ ability to achieve compliance benefits, as well as supplementary benefits will, in effect, have some form of influence on their competitive positioning. Viewed from the perspective of supplementary benefits, it may be sensible to assume that this type of benefit may positively influence banking institutions’ competitive positioning. This is arising from their deliberate decision to deploy a broader
approach to regulatory compliance (by, for example, incorporating supplementary business related requirements within their compliance efforts). Nevertheless, as mentioned earlier, it is also predicted that banking institutions’ success in attaining compliance benefits, may in one way or another, affect their competitive positioning as well. This could be attributed to the possible distinctiveness of each institution’s compliance efforts to efficiently and effectively reduce compliance cost, which may be significantly different with the initiatives deployed by other banking institutions, and therefore presents the opportunity to uniquely influence the organisation’s competitive positioning.

3.4.2. IS Capabilities for Regulatory Requirements

In relation to the type of capabilities to be utilised in the research, the work conducted by Wade and Hulland (2004) has indeed provided interesting insights into the list of IS capabilities that could be useful in measuring the value of IT investments for organisations. Therefore, in the effort to ascertain the potential contribution of regulatory system implementations, the same set of capabilities merits to be equally employed as the basis in the assessment from this particular context. In this regard, the research aims to specifically determine in what way that these capabilities are being used in accomplishing both compliance benefits, as well as the likelihood of supplementary benefits. In other words, the research aimed to discover the role of capabilities in providing crucial competencies that enable cost-effective regulatory compliance and achieve compliance benefits, as well as influence the achievement of supplementary benefits. In addition, this research also aspire to appreciate any instances of banking institution’s competitive positioning being positively influenced, arising from the accomplishment of compliance benefits, as well as supplementary benefits.

Nevertheless, it is important to note at this juncture that the definitions of IS capabilities suggested by Wade and Hulland (2004) are not meant to suit the specific purpose of regulatory compliance. Rather, they are more inclined towards
corresponding with the mainstream IT systems that are established to directly benefit organisation’s business or improve organisational revenue. Therefore, some adjustments and alterations to their original definitions had to be done (but nevertheless, will still mimic their original statements) in order to be compatible with the specific regulatory related nature of this research.

The revised definition on IS capabilities is required due to the lack of similar studies that could provide useful insights into the capabilities that are specifically associated with regulatory compliance. They are also needed to further point towards the possibility of influencing organisation’s competitive positioning through the activities of abiding by the regulatory requirements being imposed. It may be essential to note that the amended definition of capabilities tends to be universal in nature and did not attempt to limit the usage of these capabilities exclusively to the IT function of the organisation. Rather, they are meant to adopt an enterprise-wide perspective that incorporates all stakeholders who may have played a role in utilising these capabilities.

It may be worth to note further that even though the suggested definition for each IS capability had to be altered, the three classifications of IS capabilities initially mentioned in Section 2.3.3 (i.e. outside-in; inside-out; and spanning) will be utilised in this research without further modifications to their original definitions. The decision to use these given definitions arises from the comprehension that the suggested classifications of IS capabilities are meant to be used as one of the approaches to view and appreciate IS capabilities (Wade and Hulland, 2004, Day, 1994). Therefore, they will be regarded as a form of a general description for a list of capabilities that could naturally be placed in a specific group, and thus can be universally applied within the context of this study.

The eight IS capabilities proposed by Wade and Hulland (2004), listed according to the three categorisations, can be summarised as follows:

- **Outside-In** capabilities: external relationship management (ERM); and market responsiveness (MR);
- **Inside-Out** capabilities: IS infrastructure (ISI); IS technical skills (ISTS); IS development (ISD); and cost-effective IS operations (CEISO); and
• *Spanning* capabilities: IS-business partnerships (ISBP); and IS planning and change management (ISPCM).

The list of IS capabilities, outlined by their original definitions, as well as the adopted definitions that have been conceptualised as per the specific context of this research, is provided in Table 3-2 below. While the original definitions are primarily based on Wade and Hulland’s (2004) work, it is useful to appreciate that insights from other researchers that have provided the contextual background to these definitions have also been noted and taken into consideration as well.

**Table 3-2: IS Capabilities – Original and Adopted Definitions**

<table>
<thead>
<tr>
<th>Category</th>
<th>Name</th>
<th>Original Definition</th>
<th>Adopted Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outside-In</td>
<td>External Relationship Management (ERM)</td>
<td>Ability to manage the relationships between IS function and external stakeholders e.g. suppliers and outsourcing partners (Wade and Hulland, 2004, Feeny and Willcocks, 1998, Benjamin and Levinson, 1993).</td>
<td>Ability to manage relationships with external stakeholders, where necessary assistance, cooperation and information are required to be obtained in order to facilitate effective regulatory compliance.</td>
</tr>
<tr>
<td></td>
<td>Market Responsiveness (MR)</td>
<td>Ability to collect and disseminate information from external sources and respond promptly to market changes (Wade and Hulland, 2004, Bharadwaj, 2000, Feeny and Ives, 1990, Zaheer and Zaheer, 1997, Day, 1994, Kohli and Jaworski, 1990).</td>
<td>Ability to collect and disseminate information (i.e. including information pertaining to threats and opportunities) obtained from external sources, and accordingly responds to any regulatory changes.</td>
</tr>
<tr>
<td>Inside-Out</td>
<td>IS Infrastructure (ISI)</td>
<td>Ability to establish appropriate technological infrastructure that effectively accommodate organisational systems and applications (Wade and Hulland, 2004, Doherty and Terry, 2009).</td>
<td>Ability to establish appropriate technological infrastructure that effectively facilitates compliance to regulatory requirements.</td>
</tr>
<tr>
<td></td>
<td>IS Technical Skills (ISTS)</td>
<td>Ability of IT staff to acquire, deploy and manage knowledge of IS technical skills to ensure effective IT deployment and operations (Wade and Hulland, 2004, Doherty and Terry, 2009).</td>
<td>Ability of organisational IT staff to acquire, deploy and manage knowledge of IS technical skills that ensure effective IT deployment and operations that facilitate regulatory compliance.</td>
</tr>
<tr>
<td></td>
<td>IS Development (ISD)</td>
<td>Ability to swiftly develop and implement IT applications that are effective and taking advantage of new advances in technology (Wade and Hulland, 2004, Doherty and Terry, 2009, Zaheer and Zaheer, 1997).</td>
<td>Ability to swiftly develop and implement IT solutions that are effectively addressing new or revised regulatory requirements.</td>
</tr>
</tbody>
</table>
Chapter 3: Research Objectives and Framework

<table>
<thead>
<tr>
<th>Category</th>
<th>Name</th>
<th>Original Definition</th>
<th>Adopted Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost-Effective IS Operations (CEISO)</td>
<td>Ability to continually provide efficient and cost-effective IS operations (Wade and Hulland, 2004).</td>
<td>Ability to continually provide efficient and cost-effective IS operations that facilitate compliance to regulatory requirements.</td>
<td></td>
</tr>
<tr>
<td>Spanning</td>
<td>IS-Business Partnerships (ISBP)</td>
<td>Ability to integrate and align IS function with other functional areas within the organisation (Wade and Hulland, 2004).</td>
<td>Ability to integrate and align IS function with other functional areas within the organisation in order to assist in the compliance efforts.</td>
</tr>
<tr>
<td></td>
<td>IS Planning and Change Management (ISPCM)</td>
<td>Ability to anticipate future changes and growth by planning, managing and using appropriate technology (Wade and Hulland, 2004).</td>
<td>Ability to anticipate future changes and expansions arising from new or amended regulatory demands, by planning, managing and using appropriate technology.</td>
</tr>
</tbody>
</table>

As can be seen in the adopted definition column in Table 3-2, within the *Outside-In* category of IS capabilities, the External Relationship Management (ERM) capability from the perspective of this research provides the ability to manage relationships with stakeholders that are beyond the boundary of the organisation. In this regard, interactions with these external stakeholders are needed to ensure the obtainment of information, assistance, as well as cooperation that may necessarily be required to ensure the implementation of efficient regulatory compliance activities. The second type of capability within the same category i.e. Market Responsiveness (MR) on the other hand, provides the ability to collect and disseminate information obtained from external sources, which includes information pertaining to threats, as well as opportunities. In addition to this, the MR capability also provides organisations with the ability to respond accordingly to any regulatory changes that may arise. Therefore, the MR capability may present the ability to recommend optional enhancements to be implemented within the organisational regulatory IT implementations, especially arising from the activity to monitor external threats and opportunities.

With regard to the four capabilities that are classified under *Inside-Out* category, the IS Infrastructure (ISI) capability from the context of regulatory compliance provides the ability to establish appropriate technological infrastructure that effectively facilitates compliance to regulatory requirements. Hence, this capability represents the organisation’s ability to establish the needed IT solutions that allow timely
Chapter 3: Research Objectives and Framework

generation of the required information, analysis and detection. In contrast, IS Technical Skills (ISTS) from the perspective of regulatory requirements relates to the ability of organisational IT staff to acquire, deploy and manage knowledge of IS technical skills that are specifically required to ensure smooth deployments and operations of regulatory IT implementations. Meanwhile, the IS Development (ISD) capability from the standpoint of this study denotes the ability to speedily develop and implement IT solutions that are needed to effectively address any new or revised regulatory requirements. And lastly, Cost-Effective IS Operations (CEISO) capability provides organisations with ability to continually provide efficient IS operations that enable effective compliance to regulatory requirements.

In relation to Spanning category of capabilities, the IS-business partnerships (ISBP) capability in the context of this research provides the ability to integrate and align IS function with other organisation’s functional areas in the effort to assist in the compliance efforts. In this regard the ISBP capability can be used to obtain related information and cooperation from other internal functional areas in order to allow the IS function to aid in the compliance efforts. The second capability in this final category, i.e. IS planning and change management (ISPCM) on the other hand, caters for the organisation’s ability to anticipate any future changes and expansions. These changes and expansions may be attributed to new or amended regulatory demands, which are to be implemented through planning, managing and using appropriate technology.

Having appreciated the above, it is interesting to observe from the above original (and adopted) definitions that the inside-out classification of capabilities is seen to be more inclined towards emphasising the technical competencies aspects of IT. Therefore, from the specific context of this research, the discussion on this type of capabilities will be focusing on the capabilities primarily exhibited by the banking institutions’ IT departments. This particular situation can be contrasted with the appreciation on the definitions for the rest of the categorisations of capabilities (i.e. outside-in and spanning). In this regard, their classifications are seen to instead leaning towards the perspective of a broader organisational general competencies that need to be demonstrated by the IS functions of these organisations.
Chapter 3: Research Objectives and Framework

It may be useful to explain the utilisation and employment of these capabilities by banking institutions’ IT departments, as well as their relationships to the attainment of compliance and supplementary benefits. Nevertheless, this research will also be exploring the employment of similar capabilities potentially by other departments within the organisation in the effort to achieve comparable objectives.

3.4.3. Attributes of Competitive Positioning

Further to the understanding on the definition on IS capabilities and the appreciation on the alterations needed in order to suit the specific context of this research, it is also important to recognise that these capabilities posses certain number of attributes that will influence the attainment of competitive advantage and its sustainment over time. Drawing further on Wade and Hulland’s (2004) work, it was suggested that competitive advantage can be achieved through capabilities that have shown the characteristics of valuable; rarity; and appropriability, albeit most likely to be only short-lived. Nevertheless, if the organisation is able to protect these resources against imitation; transfer; or substitution, competitive advantage can be lasting or sustained over longer periods. Sustained competitive advantage in this respect does not imply an everlasting experience, but rather pointing towards to the notion that it will not be competed away via simultaneous duplication strategies from large number of competing firms (Barney, 1991, Mata et al., 1995).

Exploring deeper into the meaning of each attribute for the attainment of competitive advantage, a capability is said to be valuable if it allows the implementation of strategies that enhance organisational efficiency and effectiveness (Wade and Hulland, 2004, Barney, 1991, Ray et al., 2005). Meanwhile, rarity refers to the situation where the capability is not in plentiful supply or made accessible to a large number of organisations at the same time (Wade and Hulland, 2004, Amit and Schoemaker, 1993). Appropriability, on the other hand, refers to its ability to provide returns to the organisation, accruing from the advantage (Collis and Montgomery, 1995, Wade and Hulland, 2004, Amit and Schoemaker, 1993, Grant, 1991).
Meanwhile, in relation to the attributes that facilitate the *sustainment* of competitive advantage, an organisation is said to be able to defend its competitive advantage if its capability can be prevented from being imitated by competitors (Wade and Hulland, 2004). Prevention from imitation or low *imitability* attribute of a capability can be due to the following:

- Unique history of the organisation (i.e. where the situation is no longer available for competitors to duplicate);
- Causal ambiguity (i.e. when competitors could not clearly understand or obtain clarity on what or how to duplicate in order to achieve competitive advantage); and
- Social complexity (i.e. when complicated quality relationships exist within the organisation, and the organisation with key stakeholders, that have evolved over time) (Barney, 1991, Wade and Hulland, 2004, Mata et al., 1995).

Furthermore, a capability having low *substitutability* is said to be associated with the attributes of hardly any rare and inimitable alternative resources that can be used as replacements (Wade and Hulland, 2004, Amit and Schoemaker, 1993, Black and Boal, 1994, Collis and Montgomery, 1995). Lastly, attributes of low *mobility* is achieved when the capability is not available to be easily bought and sold as compared to other resources (Wade and Hulland, 2004).

Having appreciated the attributes that influence the *attainment* of competitive advantage and its *sustainment* over time, it is critical to further understand at this point on the application of the above suggestions by Wade and Hulland (2004) in relation to the specific context of this research. In this regard, the anticipated positive influence on competitive positioning through the achievement of the associated benefits is not implying that the associated capabilities have indeed provided a clear competitive advantage, and therefore “establishes a gap through becoming a market leader” (Doherty and Terry, 2009). Rather, it is more inclined towards showcasing the significance of the associated capabilities in attaining these benefits. Therefore, in view of the differentiated approach adopted by this research, the assessment of the *valuable; rarity; and appropriability* attributes will be differently applied. In this
regard, they will denote the possibility of organisation achieving *improved competitive positioning* [i.e. borrowing the term suggested by Doherty and Terry (2009)], rather than to indicate a distinct situation denoting the achievement of competitive advantage.

3.5. **CONCLUDING REMARKS**

This chapter have attempted to provide insights and justifications on the identified research gaps, research objectives, as well as the conceptual research framework that are to be utilised and adopted by this research. Both the research objectives and the conceptual research framework had structurally addressed the identified research gaps, and provided the justifications for the knowledge that it is trying to enhance. The chapter that follows will proceed to present the research design and methodology to be used by this research, as well as to provide the rationale for selecting them.
4.1. INTRODUCTION

Having appreciated the research objectives and conceptual research framework, this chapter will continue with the discussion by focusing on the overall research strategy, design and methodology to be adopted in the study. It is paramount to utilise an appropriate research design and deploy a good research methodology in order to help ensuring meaningful research results. Research design outlines the foundation for collecting and analysing research data. In addition, it also facilitates the generation of evidence that suits both the research questions and the set of criteria used to evaluate the research. On the other hand, a research method is to basically cater for the technique on how the research data are to be gathered and analysed (Bryman, 2008).

This chapter is generally divided into several broad sections, with an initial presentation of the philosophical standpoint adopted on this research project. Subsequently, it provides the justification for the adopted research strategy, outlining the rationale for choosing one approach over another (i.e. qualitative, as compared to the quantitative perspective). This is then followed by the discussion on the research design and methodology used by the research. In addition to these main sections, the chapter will also provide acknowledgement on the possible constraints and limitations that are affecting the research, as well as presenting the associated ethical considerations that need to be taken into consideration.
4.2. PHILOSOPHICAL STANDPOINT

As mentioned in the preceding chapter, this research generally aims to appreciate the notion of benefits and the associated capabilities arising from the implementation of regulatory IT systems in banking institutions. In order to explain the nature of relationship between theory and the research that will be undertaken, it may be worth noting that this study will have an inclination towards adopting an inductive approach to social research. An inductive perspective, in this regard, is achieved when a theory is considered as one of the outcomes by a research that has been conducted. Furthermore, this particular perspective is also typically associated with social research that is adopting the qualitative approach (Bryman, 2008). With specific relation to this study, it will seek to appreciate any instances of benefits and associated capabilities that may be experienced by banking institutions, and subsequently attempt to provide a structured explanation [or at least an “empirical generalisation” (Bryman, 2008: p. 12)] on how these possible benefits can actually be attained. However, it is important to note that this research will view the inductive approach “as tendencies rather than as a hard-and-fast distinction” (Bryman, 2008: p. 13), especially when contrasting this approach to the alternate perspectives, i.e. the deductive approach.³

Meanwhile, in relation to the epistemological considerations, this research will tend to follow the interpretivist approach. The term epistemology here refers to the philosophical theory of knowledge, particularly highlighting the opinion on knowledge that can be considered as acceptable to social researchers (Bryman, 2008). Therefore, an interpretivism perspective of epistemological position in this regard involves the explanation of the subjective interpretations of social actions, i.e. understanding the social world by appreciating the interpretations of the participants. In addition, this situation arises from further appreciation that the subject matter in social research (i.e. people and their institutions) is said to be of a different nature from the ones

³ In general, a deductive orientation occurs when a research is rooted on a theoretical perspective that subsequently guide the hypothesis adopted by the research, as well as the collection of research data. Findings that have been uncovered will then be used to reject or confirm the initial hypothesis, and may even lead to revision of the theory. A deductive approach is commonly linked to a social research that is quantitative in nature (Bryman, 2008).
employed in natural sciences. This approach is in contrast to the positivist perspective of epistemological orientation, in which, promotes the utilisation of methods from the natural sciences to be used within the context of social research (Bryman, 2008).

Furthermore, with regard to the social ontological considerations, this research will have the tendency to adopt the constructivist approach, as opposed to the objectivist perspective. Constructionism, in this context, refers to the situation where the social phenomena and their interpretations are being continually attained by social actors, i.e. arising from the interactions between individuals. This is in contrast to the objectivism position that stressed the social phenomena and their interpretations have existed independently, and beyond the reach and influence of the social actors (Bryman, 2008). In specific relation to this research, it can therefore be envisaged that while regulatory requirements will shape and confine the actions of social actors in ensuring compliance to regulatory requirements, potential interactions among individuals or departments may lead to the attainment of benefits that could positively impacting banking business. Therefore, the constructionism approach acknowledges the “ongoing accomplishment of social actors” (Bryman, 2008: p. 20) in achieving benefits beyond mere regulatory compliance activities, rather than being constrained by the requirements and only accomplishing the basic and intended regulatory outputs.

4.3. RESEARCH STRATEGY

4.3.1. Qualitative Versus Quantitative

A research strategy outlines the general approach in deploying a social research. In relation to the three areas of philosophical positions discussed earlier (i.e. linkage between theory and research; epistemological; as well as ontological considerations), differential perspectives usually arises when they are applied within the context of either qualitative or quantitative typed of social research. A qualitative research strategy typically concentrates on words rather than measurements when collecting and analysing research data (Miles and Huberman, 1994, Bryman, 2008, Bryman and Bell, 2003). As mentioned earlier, this study has the inclination to utilise the inductive
approach to social research. Furthermore, it tends to adopt the interpretivism perspective; as well as constructionism orientation. This particular situation will be in contrast to the quantitative standpoint, which is typically a research strategy that focuses on quantification during data collection and analysis. A quantitative research strategy will tend to be using the deductive approach; as well as applying the positivism and objectivism philosophical orientations. However, it needs to be appreciated that the above distinctions in philosophical standpoints are not meant to be rigid, but rather can be flexibly applied between the two contrasting research strategies (Bryman, 2008).

The debate on whether quantitative or qualitative assessment is considered to be a better option for measuring IT benefits has been discussed by several IS researchers (e.g. Bharadwaj et al., 1999, Mahmood and Mann, 2000, Chan, 2000, Chau et al., 2007). In the past, IT benefits were said to be measured primarily using the quantitative “cost reduction” approach such as reduced labour and increased throughput (Bharadwaj et al., 1999). Some researchers had argued that qualitative assessments can only be employed if quantitative measures of IT benefits are firstly agreed at the outset (Mahmood and Mann, 2000). Furthermore, in relation to the qualitative approach, many researchers have some reservations about the utilisation of perceptual assessments as respondents may not necessarily state what they believe or do what they have claimed (Seddon, 1997, Chau et al., 2007).

In contrast to the above argument, reliance on financial data has, been argued as one of the reasons why traditional analyses of IT benefits have not been very successful (Mahmood and Mann, 2000, Chan, 2000). Therefore, a more balanced view of IT value is encouraged, in a effort to gain better insights and meaningful analysis (Chan, 2000), as well as identifying possible "hidden costs and benefits" (Mahmood and Mann, 2000). In addition, collecting the associated measurements on IT investments is said to be difficult as firms are either not tracking their data or not willing to divulge them (Mahmood and Mann, 1993). Furthermore, IT investments may take several years to achieve payback (Bharadwaj et al., 1999). Even when benefits are detected, it may be difficult to differentiate the explicit contribution of IT, as the superior results attained
by organisations may have indeed been achieved by coupling IT with business investment decisions (Bharadwaj et al., 1999).

In a similar vein, Chau et al. (2007) argue that IT value involves value judgment and perceptual evaluation (such as, decision quality and better alignment with business strategies, etc.) and may not always be well-captured via quantitative measures. Bharadwaj et al. (1999) also highlighted that, based on evidence from case studies and interviews with senior management, intangible dimensions (such as improved customer service; better flexibility; and higher product and service qualities) were in effect, cited as among the key improvements from IT investments, and thus provide a much more extensive view of IT benefits. In this regard, Chan (2000) has also called for renewed recognition of the important contributions of qualitative assessments, through addressing the “soft” IT value measures in an IS research, as compared to the “hard numbers” or the quantitative perspective.

Mahmood and Mann (2000) have also indicated that quite a number of IS research studies have indeed been utilising qualitative approaches, and therefore there is an opportunity for both groups in IT productivity research to contribute, as well as to ideally complement one another. Meanwhile, in specific relation to regulatory compliance, Hupkes et al. (2008: p. 249) have also interestingly suggested that one of the broad approaches in assessing the impact of regulation would be by relying on qualitative assessments which “descriptively evaluates the positive and negative effects of regulation.”

With regard to this study, it is anticipated that difficulties may arise if quantitative indicators are to be used to assess possible value of IT investments, which have been implemented for regulatory purposes. This situation can be attributed to the earlier understanding where regulatory related IT investments are most likely not being established to directly benefit organisation’s business, improve revenue, or enhance business efficiencies. Therefore, quantitative measurements that could be used to gauge possible IT benefits may not be feasible in the context of regulatory IT implementations, attributing to their potential absence. Furthermore, it should be emphasised that few studies can be regarded to have truly attempted to empirically
investigate organisation’s regulatory IT implementations from the context of potential benefits, as well as the required capabilities [see Chapter 2]. In a situation where there are very few or virtually no previous research that had made an effort to empirically examine the area of interest, an exploratory perspective (e.g. Bowen, 2005) using the qualitative approach is regarded to be more viable and practicable solution. In this regard, a quantitative approach may be difficult and complicated to deploy, arising from the lack of prior research to facilitate the establishment of a reasonable foundation or basis for the intended research (Bryman, 2008).

Hence, in view of these important considerations, as well as taking into account the viewpoints from the literature presented earlier, it would seem sensible to conduct this study utilising a qualitative strategy. This standpoint also takes into account the perceptual measures that would be an important avenue to explain the possible notion of leveraging regulatory IT investments to benefit the organisation.

Indeed, qualitative research approach can, in effect, be used to obtain in-depth and richer understanding, such as the thought processes and experiences which would be difficult to extract through alternative research methods (Strauss and Corbin, 1990, Bowen, 2005, Wardle, 2002). Importantly, Myers (1997) highlighted that research using qualitative dimensions has progressively become more useful as the spotlight of IS research moved from technological to managerial and organisational issues. Similarly, Johnson et al. (2006) have also emphasised that qualitative research has indeed made a significant contribution to the areas of management research for many years. In addition, Bryman (2008) has further highlighted that qualitative research approach has becoming increasingly popular among social researchers.

It may be worth noting at this juncture that by utilising qualitative assessments, this study will further distinguish itself from previous work of some IS researchers. More specifically, Krell and Matook (2009) had employed a quantitative perspective in their effort to assess possible competitive advantages arising from the utilisation of formal planning methods in regulatory compliance efforts. This research will also be using primary data mainly collected through the interview approach, and therefore will not be relying on a secondary dataset as per Krell and Matook’s (2009) study.
**4.4. RESEARCH DESIGN**

A research design offers guiding principles for collecting and analysing research data that allows empirical evidence to be generated. This section will provide the justification for adopting the chosen research design. In addition, it will also present the approach that can be taken to assess the quality of the research, based on the research strategy and design that have been adopted by the study.

**4.4.1. Rationale for the Adopted Research Design**

In order to justify the selection of the research design that is most suitable for the study, various design possibilities need to be firstly comprehended and appreciated. In this regard, the discussion will be concentrating on the five principal research designs, as suggested by Bryman (2008), i.e.; experimental design; cross-sectional design; longitudinal design; case study design; and comparative design. The nature of and differences between these research designs are briefly elaborated in the following discussions:

- **Experimental Design**: is a research design that is widely known as true experiments, and is usually done in a laboratory (i.e. laboratory experiments) or on the field (i.e. field experiments). In a true experiment, the independent variable typically needs to be manipulated in order to ascertain whether it has any influence on the dependent variable. Nevertheless, manipulation of independent variables in the context of social research is usually not possible. For instance, the classification of male or female could not be manipulated so that a research participant’s gender is altered to suit the alternative. Hence, this type of research design is said to be rarely utilised in social research environment;

- **Cross-sectional Design**: is a research design that is primarily utilised when a researcher is interested to understand the variations between two or more cases. Quantitative or quantifiable data relating to several variables is usually collected from several cases, via questionnaire or through structured interview, at an almost simultaneously timing. In a qualitative research, this type of research design will
usually employ unstructured or semi-structured interviewing with a number of research participants, being conducted at a particular time frame;

- **Longitudinal Design:** is a research design which is commonly used as an extension of survey research (i.e. by using self-completed questionnaire or through a structured interview approach) typically within a cross-sectional orientation. Usually a sample is surveyed, and subsequently being surveyed again at least in another separate occasion. Longitudinal designed social research usually employs a *panel study* (i.e. where sample is randomly selected in at a national scope, such as organisations, schools, etc.) and a *cohort study* (i.e. a focused data collection e.g. people with similar characteristics). Both panel and cohort studies are designed to show social change and appreciate causal relationships over time;

- **Case Study Design:** is a comprehensive and intensive analysis of a particular case (such as a community or organisation), in which the researcher is aiming to appreciate the complexity and the nature of the case (Stake, 1995). Case study approach is usually associated with qualitative research (due to the utilisation of participant observation and unstructured interview methods), since they help to provide intensive and detailed insights into a specific case. Critiques of case study design highlighted that outcomes of the research is not generalisable. Nevertheless, investigators adopting this research approach advocate that it is not the original intention for them to generalise their studies on other possible cases. Furthermore, it is said that their main intention is to ensure how well the researchers would be able to develop a theory from the outcome of the research (Mitchell, 1983, Yin, 2003);

- **Comparative Design:** is a research that studies two or more different cases through the utilisation of a similar research approach and instrument.\(^4\) The comparative perspective in this type of research design is implying that the understanding of social phenomena would be more effective when they are differentiated with contrasting situations. Researchers employing this approach are aiming to obtain insights into possible *similarities* and *differences*, or to gain

\(^4\) Examples of research instrument include an unstructured; as well as structured interview styles (Bryman, 2008).
better understanding of social reality in different contexts. Within the domain of qualitative research, comparative design will usually employ a multiple-case study approach. Several researchers (e.g. Miles and Huberman, 1994, Bryman, 2008) have highlighted that in recent years, a number of qualitative researchers have lean towards the utilisation of more than one case study. By contrasting two or more cases, researchers will be in a better position to ascertain the situation where a theory will be feasible or otherwise (Eisenhardt, 1989, Yin, 2003).

Having presented the five key research designs, it is worth noting that this study will be utilising the *qualitative* perspective, in order to uncover any possible value (and the associated capabilities) from banking institutions’ regulatory IT investments. Therefore, arising from the understanding on possible research designs that could be suitable for a research from the qualitative orientation, a *cross-sectional design* seemed to be the best approach to be adopted by the study.

The decision to utilise such a design arises from the understanding that while the notion of benefits may be credible arising from the review of the literature [see Chapter 2], there could always be instances where such benefits may not be detectable. Furthermore, the decision can also be attributed to the earlier appreciation [see Section 4.3.1] on a situation where there are virtually no similar previous empirical research being conducted on the area of interest. Therefore, when there is lack of prior research to establish a reasonable foundation, an exploratory perspective is said to be more viable. Hence, it may be sensible for the research to explore this idea through data collection efforts conducted on several banking institutions, instead of merely concentrating on any specific, or even several organisations.

Nevertheless, it may also be reasonable to assume that the notion of benefits might eventually be detected within the banking institutions being engaged with during data collection exercise. Therefore, a plausible approach going forward would not be to continue with the exploratory approach, but rather to gain deeper explanatory insights. For that reason, in this particular stage where benefits have indeed been uncovered, the research will move to adopt a *comparative design* approach to obtain
Chapter 4: Research Strategy, Design and Methodology

richer understanding, and primarily concentrating on a smaller set of banking institutions.

Therefore, it should be noted that this research can be regarded as adopting a mixed-design approach, by firstly utilising cross-sectional, and subsequently, comparative research designs at a separate stages of the research. This approach may be in line with suggestions in the literature, which have stated that when determining the best approach that would be suitable for a research, deliberate choices need to be made on “alternating and/or combining/integrating methods as the study proceeds” (Miles and Huberman, 1994: p. 174)

Exploring further on the comparative design, this research approach may be regarded as the best option for detecting benefits within banking institutions. This situation arises from the appreciation that the approach will be able to facilitate detailed insights into possible similarities and differences between multiple case studies, as well as assist in detecting negative cases (Miles and Huberman, 1994). Furthermore, multiple cases approach will allow appreciation on the process and outcomes from many cases, which will deepen the understanding and the ability to explain on a particular condition. This situation may be attributed to local and peculiar circumstances, and thus further enable more detailed descriptions and explanations (Miles and Huberman, 1994).

Examining multiple cases may also identify specific situations that may cause a findings to occur, such as uniqueness of a particular case study arising from its developmental history (Miles and Huberman, 1994, Silverstein 1988). Moreover, it has also the inclination to discover the “underlying similarities and constant associations” (Ragin, 1987, Miles and Huberman, 1994). Similarities and associations in relation to the study may be regarded as what are being implied in relation to the benefits from regulatory IT implementations, as well as the associated capabilities needed. Additionally, one of the reasons for using multiple case studies is also to increase generalisability (Miles and Huberman, 1994). Although it has been acknowledged earlier that this motivation would not be of typical interest in a qualitative research (e.g. Denzin, 1983, Guba and Lincoln, 1981, Miles and Huberman,
researchers may nevertheless want to know the applicability of their research findings to other settings that can be regarded as similar (Miles and Huberman, 1994).

It is worth noting that differing views exist with regard to the effectiveness of comparative design (e.g. Dyer and Wilkins, 1991). In this regard, it is argued that multiple case study approach may result in the researcher paying less attention to the uniqueness of each case. The possibility of this situation occurring in this research is indeed acknowledged (i.e. in contrast to an intensive analysis of a single case study approach), and can further be attributed to the constraints of time and resources within a PhD research. However, as mentioned earlier, engaging with more than one case study will provide the strengths to obtain richer insights, primarily on the potential differences and similarities between them. Hence, through the appreciation on the possible commonality and differentiating attributes from multiple case studies, it is envisaged that this research design would be able to present a good foundation for potential theory building. As supported by Bryman (2008: p. 61), “the key to the comparative design is its ability to allow the distinguishing characteristics of two or more cases to act as a springboard for theoretical reflections about contrasting findings.”

4.4.2. Quality Criteria for Qualitative Research

Moving the discussion to the quality criteria, there are wide discussions and contrasting views in the literature regarding the assessment of reliability and validity of qualitative research (e.g. Mason, 1996, Lincoln and Guba, 1985, Guba and Lincoln, 1994, LeCompte and Goetz, 1982). Therefore, detailed evaluation on which perspective is more appropriate as compared to the other would be beyond the scope of this study. Nevertheless, it is beneficial to briefly note the main highlights in the discussions as have been related by Bryman (2008), before presenting the approach that may be the most suitable option for this research.

One particular line of thinking to assess the quality of qualitative research is by adapting the assessments on reliability, validity and generalisability from the
Chapter 4: Research Strategy, Design and Methodology

quantitative perspective, but nevertheless by understating the importance of measurement (e.g. Kirk and Miller, 1986, Mason, 1996, LeCompte and Goetz, 1982). Although the context of measurement is being considered as one of the significant criterion in assessing the quality of quantitative research, it is in effect, not a primary concern from the qualitative researchers’ perspective. Therefore, this particular view suggests that quality assessments similar to quantitative research can be utilised provided that the measurement perspective is given a lesser prominence.

Other researchers have suggested a set of alternative and differing criteria (as opposed to the ones being utilised by quantitative researchers) that are to be used by qualitative researchers (e.g. Lincoln and Guba, 1985, Guba and Lincoln, 1994). For instance, instead of using the measurement of reliability, validity and generalisabilty, it was suggested that a qualitative research be evaluated from the perspectives of trustworthiness (i.e. credibility; transferability; dependability; and confirmability), as well as authenticity (Lincoln and Guba, 1985, Guba and Lincoln, 1994).

However, the evaluation using these criteria is not without contention. As reflected in the evaluation for the credibility criterion through respondent validation\(^5\), there may be a risk of research participants becoming defensive or even request for censorship to be applied to the findings that have been revealed to them. This is over and above to the understanding that research participants may not even have the ability to appreciate the research findings in the first place, arising from the development of concepts and theories that are typically an output of qualitative research. Furthermore, the auditing approach suggested for the dependability criterion (i.e. to ensure complete research records are kept for all phases of the research) may be difficult and demanding to implement in practice due to the large data sets usually being generated in a qualitative research (Bryman, 2008).

Additionally, to expand the discussion on the already diverse suggestions in assessing the quality of qualitative research, in recent years, further alternative evaluation schemes had also been proposed (e.g. Yardley, 2000). For instance, it was

\(^5\) Respondent validation (or member validation) in this context is a process where the researcher provides the findings of the research to the research participants with the intention to solicit feedback from them (Bryman, 2008).
recommended that the quality assessment be done from the perspectives of; sensitivity to context; commitment and rigour; transparency and coherence; and impact and importance (Yardley, 2000).

Fortunately there is a compromise position assessing the quality of qualitative research, i.e. in between the tendency to use criteria for quantitative research and the utilisation of alternative or different criteria as described in the preceding paragraphs. This view by Hammersley (1992) suggests that validity of the findings must be plausible and credible, and should take into consideration the amount and the type of evidence to support them. Therefore, the main consideration to judge the validity of a qualitative research in this context is to be done via the plausibility and credibility of a researcher’s findings, on the basis of sufficiency of supporting evidence (Hammersley, 1992). This approach is taken arising from the acknowledgement that “we can never be absolutely certain about the truth of any account, since we have no completely incontrovertible way of gaining direct access to the reality on which it is based” (Bryman, 2008: p. 382).

In a nutshell, there is a recognition, that a direct application of quantitative research criteria, in the context of qualitative research, is neither attractive nor desirable. Nevertheless, according to Bryman (2008), most qualitative researchers nowadays will tend to adopt the compromise position, although not necessarily approving the views from Hammersley (1992). Therefore, without totally ignoring the alternative assessment criteria suggested in the extant literature, this research will primarily be rooted on this position in the effort to assess the validity of this research.

4.5. RESEARCH METHODOLOGY

A research methodology outlines the techniques to be used for the collection and analysis of research data. In this regard, this section will provide a discussion on how data for the research are sampled, gathered and analysed. The rationale for utilising a specific technique, together with its associated theoretical reasoning will be correspondingly presented. In addition, the decision for selecting the location of study is also discussed accordingly.
4.5.1. Gathering and Sampling of Data

The interview approach has been considered as a major source of research data in an interpretive study\(^6\) (e.g. Doherty et al., 2006, Walsham, 1995). An interview is a real-time conversation, using approaches that ranges from structured interviews to unstructured or open-ended questions (Mingers, 2003). However, it has been suggested that interviews conducted within a qualitative study will tend to be less structured, as they aim to gain detailed views or insights from the interviewees. In contrast, interviews adopted in quantitative research are said to be more structured, in order to “*maximise the reliability and validity of measurement of key concepts*” (Bryman, 2008: p. 437). Therefore, interviews in a qualitative research will have the tendency to be flexible, and typically guided by the direction of information being revealed by the interviewee. Nevertheless, it is important to appreciate that interviews conducted need to be done in a way that they do not lose sight of the intended research goals and objectives. In qualitative interviewing, rich and detailed response is typically sought, and the interviewee may be interviewed more than one occasion (Bryman, 2008).

In line with the above view, this research will adopt the semi-structured interview, similar to the approach that had been utilised by several IS researchers (e.g. Hu et al., 2007, Doherty et al., 2006, Doherty et al., 2012). This specific approach is in harmony with the suggestion that a researcher with a fairly clear focus, as opposed to the ones with just a general idea of research, would tend to use semi-structured interviews, as more explicit areas or issues would be able to be addressed (Bryman, 2008). In a semi-structured interview, the researcher will usually be guided by an interview guide that contains a list of questions or topics to be covered.

With regard to the design of the interview guide, the research objectives that have been identified earlier [see Section 3.3] will be used to define the information that needs to be solicited from the interviewees. Therefore, the list of semi-structured interview questions to be asked, or issues to be addressed, during the data collection

\(^6\) As highlighted earlier, an interpretive study can be regarded as having the inclination towards understanding the social world by appreciating the interpretations of the participants. An interpretivist perspective tends to be associated with social research that is adopting the qualitative approach.
exercise, should be able to provide assurance that allows each research objective to be fully explored. Using these research objectives as a guide, a list of provisional interview questions will be developed, and will subsequently be tested and further be refined during a pilot interview exercise [see Section 5.2.1]. However, it is important to note that the usage of an interview guide does not imply that the line of questioning will need to strictly follow the sequence outlined in the guide (Fielding, 1993). Still, all questions in the guide should generally be asked with an almost similar wording in all interviews (Bryman, 2008). In addition to the semi-structured interview line of enquiry, open ended questions (e.g. Hu et al., 2007) will nevertheless be utilised as well, especially in a situation where a more detailed explanation is to be solicited from the interviewees.

In relation to the discussion on the sampling of data, most qualitative researchers have recommended the usage of purposive sampling (Bryman, 2008). Purposive sampling in this context is where the sampling is based on the number of people that are relevant to the areas of interest and of whom the researcher wanted to interview. Therefore, selection of sample in purposive sampling approach is not to be done randomly, and thus will not allow the researcher to generalise to the overall population. Nevertheless, this approach concurs with Bowen’s (2005) suggestion that qualitative research emphasises on quality rather than quantity by having in-depth understanding on a small number of respondents. In specific relation to the research, one type of purposive sampling, i.e. the snowball sampling will be adopted. A snowball sample is a non-probability sample where initial contacts with a small number of individuals that are relevant to the research are made. Accordingly, these initial contacts will subsequently be used to extend the interactions with other individuals that could later on be identified as potential research participants (Bryman, 2008).

Furthermore, in addition to the above guiding principles, it was also suggested that a sample selected using the purposive sampling approach would normally provide good variety, in which sample members will differ from each other in terms of their key characteristics (Bryman, 2008). In view of this suggestion, this research will be
targeting three general categories of research participants in the banking institutions. The first category will be members of staff from the Compliance department, who are typically made responsible for the implementation of organisation’s activities that relate to the management of regulatory requirements. Meanwhile, the second category of research participant will comprise staff from the IT department, as they are perceived to be the key party responsible for or assisting in the implementation of regulatory IT systems in the organisation. Finally, the last category of potential research participant will be obtained from relevant business departments that are most likely to have realised business benefits from regulatory compliance activities.

As far as possible, research participants selected for this study will comprise members of staff that are of a certain seniority, such as managers (and above) who are closely related to, or being impacted by, the associated compliance activities or regulatory IT system implementations. It is suggested that IT staff who are at a certain level of seniority will be more well versed with the organisational IT capabilities and competitive positioning (Bhatt and Grover, 2005). Hence, they are therefore believed to be able to provide insights into the possible value from the implementation of regulatory IT systems. Furthermore, similar approach of interviewing staff having somewhat a senior position in the banking institution is also being applied to non-IT related staff as well. In this regard, the institution’s business related staff with at least having a managerial experience will be selected for the study. The reason for targeting this group of individuals is due to the understanding that managers are said to be the most informed person on strategic issues of IT utilisation, as well as, would be in an excellent position to evaluate IT value in their organisation (Gregor et al., 2006, Ravichandran and Lertwongsatien, 2005).

Selecting banking staff from the business side (i.e. business executives) is also important for the research as they are considered ideal to act as key informants in a qualitative assessment of IT benefits (Tallon et al., 2000, DeLone and McLean, 1992). This can be attributed to the situation where they are typically direct consumers of IT, and thus would be proficient to establish an overall perception of IT benefits based on their personal experience (Tallon et al., 2000, Davis and Olson, 1985, Rockart and
Flannery, 1983). This situation is also supported by the previous discussions regarding the literature [see Chapter 2], which have highlighted that the notion of IT value can only be unlocked by business managers, executives and users (e.g. Peppard et al., 2000, Peppard, 2007, Markus, 2004, Peppard and Ward, 2005). Moreover, since these individuals are more engaged in IT investment decisions, they are increasingly exposed to the various viewpoints regarding past IT investments performance (Tallon et al., 2000, Watson, 1990). Therefore, the research will be adopting an approach that only senior business executives would be interviewed, where possible. The reason for adopting this decision can further be credited to the suggestion by Tallon et al. (2000: p. 146) which have highlighted that “by virtue of their seniority within the corporation, business executives are in an ideal position to identify how and where IT creates value for the business.”

4.5.2. Analysis of Data

The general strategy or framework guiding the analysis of research data for this study will be premised upon the approaches of grounded theory (Strauss and Corbin, 1990, Matsuo et al., 2008, Glaser and Strauss, 1967). Grounded theory has been regarded as one of the most influential and widely used strategies for conducting qualitative data analysis (Bryman, 2008). This strategy promotes the notion that qualitative analysis should be grounded or rooted in the data, and thus has similar characteristics with the inductive approach of social research. Bryman (2008) suggested that grounded theory is not a theory by itself, but can be regarded as a set of guiding principles that outlines possible approaches in the analysis of qualitative data. In this regard, this study will adopt the two key precepts of grounded theory, in that it will seeks to: develop theory out of the data (Cresswell, 1998, Matsuo et al., 2008); and adopt an iterative approach to data analysis (Miles and Huberman, 1994).

With regard to the information gained from the interview process, the conversations with the identified research participants will be voice recorded (e.g. Matsuo et al., 2008), and then be fully transcribed verbatim. Voice recording of interviews is regarded to be more reliable and accurate than written records (Thompson, 1988).
Chapter 4: Research Strategy, Design and Methodology

will allow the interviewer to: be highly alert to what is being said; to follow-up or to further probe wherever necessary; and also to draw attention to any potential inconsistencies in the answer received. If interviews are not voice recorded, the researcher will have the tendency to be distracted by having to write down notes on what is being said and revealed (Bryman, 2008).

The transcribed interviews will be coded by reading and re-reading of the printed interview transcripts, and inserting marginal remarks, where necessary (Miles and Huberman, 1994, Bryman, 2008). Marginal remarks will be used to assist in, for example: noting what is being coded; obtaining ideas; getting new interpretations; or determining their inter-relation with other parts of the interview data (Miles and Huberman, 1994). In addition, most qualitative analysis is also said to be conducted using manual means. Repetitious efforts to manually read and re-read the interview transcripts over and over will indeed be beneficial, as they will provide familiarisation to the content, as well as understanding the tacit or underlying meaning within the data (Bryman, 2008).

In order to assist in attaining a thorough analysis, a software product called NVivo will be utilised by the study. This type of computer software is usually referred to as CAQDAS or Computer-Assisted/Aided Qualitative Data Analysis Software (Bryman, 2008). However, it is important to note that software similar to NVivo will not assist a researcher to decide how coding is to be done, or how findings are to be uncovered and interpreted (Sprokkereef et al., 1995, Weitzman and Miles, 1995). Nevertheless, there is definitely an important use of such software, as it eases the data analysis efforts arising from the large amount of research data that qualitative research usually generates. Therefore, due to the potentially overwhelming nature of qualitative data, the software is typically used by social researchers, to primarily make the tasks of coding and retrieving of data easier and faster. Software like NVivo helps a researcher to expedite the coding process; make potential alterations more flexible and efficient whenever needed; and tremendously increase the retrieval rate (Bryman, 2008).

Subsequently, key patterns and emerging themes will be identified (Bowen, 2005, Miles and Huberman, 1994). The themes that are of interest to the research will be in
Chapter 4: Research Strategy, Design and Methodology

line with the intention to gain insights arising from the identified research objectives outlined in the preceding chapter. The interview transcripts will also be constantly referred to, in order to reduce the risk of losing the contextual background or narrative of the findings. In most instances, reading the interview transcriptions helps to gain deeper insights and understanding of what an interviewee was saying. Thus the effort will be able to reduce the risk of “decontextualising data” (Fielding and Lee, 1998), as well as the possibility of being disconnected or uninvolved from the findings.

4.5.3. Location of Study

Chau et al (2007) suggest that little research on IT value has been conducted in Asia and Europe. According to these writers, one of the likely reasons for this situation to occur is because the IS discipline in these parts of the world is said to have yet reach a stage that is similar to the North America’s. Therefore, because of this, as well as the researcher’s familiarisation with the banking environment in his home country, it was decided that the research should be focused on the Malaysian banking industry. Moreover, by positioning the research in the context of Malaysia, the data collection process will also most likely be less complicated, particularly recognising the position of the researcher being a Malaysian central banker. It is indeed important to be sensitive to the nature of organisations where a researcher is trying to access (Bryman, 2008). Therefore, accessing the right individuals in the banking institutions may be tricky to an academic researcher, due to the potential hectic nature of a typical banking environment. This situation may even result in a request to conduct one-to-one interview with the bankers being declined.

However, it needs to be noted as well that the higher tendency of having smooth access to conduct interviews with the identified individuals arising from the researcher being a central banker may also pose some ethical issues to the research. As will be discussed in the subsequent section, the risk of potential research participants feeling obligated to participate in the research, or even resulting in any respondent biases, are likely to have been fully mitigated by efforts taken to address these potential issues. In addition, it may be worth briefly highlighting at this juncture
as well that not all requests to conduct interviews were indeed successful. The researcher did encounter several situations where the identified bankers had politely declined to participate, as well as experiencing the issue of non-responsiveness, even after several requests to conduct interview were made to the relevant individuals [see Section 9.5].

4.6. CONSTRAINTS AND LIMITATIONS

Being a central banker for over 20 years, the researcher’s approach in conducting this study might somehow be influenced by the years of experience and practice. It is undisputable that some form of preconceived notion may exist due to the researcher’s opinions and assertions rooted in the underlying values by being an experienced central banker. Nevertheless, efforts have been taken to ensure that the research will not be unnecessarily influenced by the aforementioned situation. In this regard, it is recognised that the research needs to be as far as possible, neutrally conducted and analysed in an unbiased view without any preset judgement. As the research is adopting an interpretive approach, it is hugely important for the researcher to be able to exhibit the skill to effectively engage, investigate and learn how possible interactions might have taken place from the viewpoints of the participants (Chen and Hirschheim, 2004).

As discussed earlier, regulatory compliance can be viewed both as a cost, as well as a potential opportunity. Given the strong views that participants might hold on this issue, then, the researcher will need to be impartial about the findings of the research and he must refrain from taking sides. This is especially important in the case when the results did not revealed the intended insights or match the research expectations regarding the possible benefits that could be attained by organisations.

Further to the above, the fact that the researcher is also a central banker who is intending to conduct a study on banking institutions which fall under the purview of the central bank, will similarly pose another possible issue of concern. Indeed, the literature suggests that qualitative researchers should be closely involved and deeply
immersed within the research process (Bowen, 2005). In addition, this particular research approach is also said to depend heavily on self-reported experience (Matsuo et al., 2008). Therefore, as the researcher can also be seen as an agent of the regulatory authority, this unique situation might raise some issue of trustworthiness from the perspective of respondent’s biases, in which respondents may, in effect, highlight what the researcher wants to hear and not what really happened (Bowen, 2005). On the other hand, there is also the risk of the researcher posing leading questions during the interview sessions and unnecessarily influence the responses from the interviewees. Leading questions are the kind of questions that tends to lead the interviewee in a particular direction and suggesting a particular reply (Bryman, 2008).

It is worth noting that the researcher may not be entirely value free, arising from his personal beliefs or feelings (Bryman, 2008), as depicted above. Nevertheless, mitigation to the concerns and matters relating to the researcher’s values, as highlighted by the earlier potential constraints and limitations (especially in respect of neutrality and impartiality), will be partially addressed by utilising interview protocols (e.g. Matsuo et al., 2008, Bowen, 2005). This effort is to particularly convince the research participants that the interview approach and the line of questions used have indeed gone through rigorous quality assessments enforced by the University. In this regard, the interview session will be conducted using an interview guide (Bowen, 2005, Matsuo et al., 2008), which will define the areas that the researcher will be covering. The usage of interview guide may also address the concern on the researcher to potentially posing leading questions during the interview sessions.

It is important to reemphasise at this juncture as well that the research is aiming to primarily understand and appreciate banking institutions’ regulatory IT implementations, which may possibly lead to the realisation of organisational benefits. In achieving this general research goal, research participants will be informed in advance that there will be no answer or response made by the interviewee that will be considered as the right or wrong approach to regulatory compliance. This will allow the researcher to effectively engage, investigate and appreciate the situation
Chapter 4: Research Strategy, Design and Methodology

affecting the participants, specifically from their point of view, as suggested by Chen and Hirschheim (2004).

Furthermore, official assurance of strict requirements to preserve respondent’s confidentiality and non-identifiably of information gathered throughout the research, could also be treated as another measure to alleviate any possible concern that may be felt by the interviewees, especially arising from the researcher being an employee of a regulatory authority. Importantly, it will also be clearly made known that the researcher will be under no obligation to report the results of the study to Bank Negara Malaysia (i.e. the Central Bank of Malaysia, in which the researcher is an employee). In effect, the regulatory authority does not have any vested interest in the outcomes of the research, even though the researcher is being financially supported by this organisation. Instead, exclusive rights to the results of the research will be solely be retained by the University where the study is initiated. In addition, all information gathered by the research will only be made available to researcher, as well as, his research supervisor. Therefore, it will be made explicitly known that no raw data will or can be shared or published to any third parties. This situation is however with one minor exception, i.e. in instances where direct interview quotes will need to be utilised in supporting of evidences or arguments. Nevertheless, it will be made known that in this particular situation, all identifying information will indeed be adequately masked and disguised accordingly.

Other constraints and limitations in the research can also be seen from the inherent nature of the chosen research sampling approach. Purposive sampling approach that will be utilised in this research will introduce some form of bias in the way how the research participants will be selected, as it was meant to primarily correspond with the target group that the researcher wanted to interview. Additionally, the chosen group of interviewees might result in an outcome that is skewed to the opinion of a selected few. However, since only members of staff of a certain seniority will be selected for this research, their views can be treated as a “valid representations of IS activities in their organisation” (Ravichandran and Lertwongsatien, 2005). It should be noted that the interviews will be conducted within the three general categories of
research participant (i.e. from the Compliance department; IT department; as well as the various business departments where benefits may likely to emerge). Therefore, by interviewing these three targeted categories of participants, the risk of the results being skewed and confined to the opinion of a particular category of research participant should somehow able to be mitigated.

4.7. ETHICAL CONSIDERATIONS

This research acknowledges that there are possible ethical problems that may unavoidably arise, and therefore emphasis on the need for them to be adequately addressed and mitigated. Within the specific context of this research, a study conducted using one-to-one interviews may be subjected to several ethical issues which may adversely affect the credibility of the research. In this regard, the discussion on ethical principles in social research is more inclined towards four significant areas, i.e.; harm to participants; informed consent; invasion of privacy; and deception (Diener and Crandall, 1978, Bryman, 2008).

This research will not employing any elements that could lead to deception; invasion to privacy; or a situation that may create harm to the research participants. Nevertheless, the research will definitely need to address the need of having informed consent, arising with the need to interact with human subjects. In this regard, by utilising the “Informed Consent Form” developed specifically for the research, participants in the interview exercise will be made fully aware about the intentions of the research. They will also be provided with enough information for them to decide whether to voluntarily participate in the research or otherwise, before the interview session can actually be initiated (Bryman, 2008). In addition, it will made explicitly clear that research participants will also be free to decline answering any of the questions being posted to them, as well being free to decide not to participate in the research any longer, at any point within the interview process. In relation to the specific contents that need to be conveyed to the potential research participants, Bowen (2005: p. 214) had suggested some basic elements that should ideally be considered:
Chapter 4: Research Strategy, Design and Methodology

“A brief description of the study and its procedures; full identification of the researcher’s identity; an assurance that participation is voluntary and that the respondent has the right to withdraw at any time without penalty; an assurance of confidentiality; and benefits and risks associated with participation in the study.”

The “Informed Consent Form” will be paired with a document known as “Participation Information Sheet”, which will be used to provide detailed explanations of the issues that need to be imparted to the participants in the research. For example, this may include information, such as: the contact details of the researcher and the research supervisor; anticipated duration of interview session; destruction of research data; etc. An Ethical Clearance Checklist will need to be completed, in line with the rules and regulations of the University, which is specifically required when research involving human participants is conducted.

As mentioned in the preceding section, it is also important to emphasise the efforts that will be taken to ensure that the information revealed, to the researcher, throughout the data collection exercise will not be directly associated with the actual identity of the interviewees. In this regard, all obtained information is to be treated as strictly confidential and be made available only to the researcher and the research supervisor. In addition, results of the research will be kept anonymous and only to be reported in a non-identifiable manner. Moreover, pseudonyms will also be employed in order to disguise the real information, where it is appropriate and essential to do so.

4.8. CONCLUDING REMARKS

This chapter has provided the rationalisation and justifications for the chosen research strategy, design and data collection approach, in the effort to empirically analyse the areas of interest identified in the previous chapter, as well as ensuring the realisation of meaningful results. This chapter has also acknowledged the possible constraints that are affecting the research, as well as ethical issues that need to be taken into consideration to ensure the credibility of the research. Next, the study will proceed to
reflect on the actual data collection exercise that has been undertaken, and issues affecting this important process. In addition, results of a preliminary analysis, which has influenced the subsequent direction of the research, will also be discussed and elaborated.
Chapter 5

Data Gathering, Initial Analysis and Background

5.1. INTRODUCTION

This chapter will proceed to present the actual data collection activities and findings from the preliminary analysis, as well as the contextual and associated information relating to AML/CFT (anti-money laundering and counter financing of terrorism). In this regard, this chapter can be seen as being broadly divided into two key sections. The first key section will elaborate the various phases of data collection exercises that have been deployed. In addition, it will also provide the rationale and motivation for focusing on AML/CFT requirements arising from the outcome of the initial findings, in which had influenced the direction of the research in exploring the specific areas of interest.

Meanwhile, the second major section will provide the contextual background information that is aimed at setting the scene for a more detailed discussion in the subsequent analysis chapters (i.e. Chapters 6 to 8). Firstly, it will discuss the universal requirements on AML/CFT, followed by highlighting the specific areas that are affecting the Malaysian banking industry. In addition, it will also present the primary components of a typical AML/CFT IT system, as well as providing brief background information on the IT systems for the two detailed case study organisations. Importantly, this section will also discuss the general assumptions and approaches adopted by the study when analysing and presenting research data. They are introduced at this juncture to allow a more specific and relevant set of assumptions and approaches to be later presented, where necessary, in each of the subsequent
Chapter 5: Data Gathering, Initial Analysis and Background

analysis chapters that follow. Lastly, the concluding remarks section provides the summary and conclusion to the chapter.

5.2. DATA GATHERING

Overall, the research can be regarded as having adopted a four stage data collection approach, with two stages being considered as the period where most of the data had been gathered, i.e. through face-to-face interview exercises. The key stages are pilot interviews, first and second data gathering, as well as the supplementary data collection exercises. The activities related to each key stage are explained in the sections that follow.

5.2.1. Pilot Interviews

The data gathering process for the research was piloted via a long distance phone interview with a member of staff from the Compliance department in one of the banking institutions in Malaysia (i.e. Bank A). The pilot interview (interview no: 001) was carried out primarily to detect any potential concerns that could emerge during the actual data collection exercise, as well as issues attributing to the usage of the interview guide [see also Section 4.5.1]. While no major problems were encountered, the interview guide was refined nevertheless in order to facilitate the clarity of questions being posted.7 Upon this enhancement process, another pilot interview (interview no: 002) with the same individual was conducted for a second time, two weeks later, using a similar method. The second follow-up interview was done so as to obtain further information and clarification of some of the matters that were discussed during the first pilot interview. Both voice recordings for the two pilot interviews were fully transcribed and reviewed prior to the subsequent key phase of the data collection activities.

7 See Appendix I for sample questions in the interview guide.
Chapter 5: Data Gathering, Initial Analysis and Background

It should be noted that another member of staff from Bank A had also been identified for the pilot interview exercise. Nevertheless, the planned interview could not be conducted, despite the numerous attempts to reach this person by phone, and given the quality of the two previous interviews, it was decided to conclude the piloting process at this stage.

5.2.2. First Phase Interviews

a) Overview

The first phase of interview exercise was conducted for a period of one month in Malaysia, subsequent to the pilot interview process. Face-to-face interviews were carried out with members of staff from various banking institutions. Nevertheless, it is important to note that during the first phase interview exercise, the two detailed case study organisations for the research (i.e. Bank A and B) had yet to be identified and selected. As already mentioned [see Section 4.4.1], this situation can be partly credited to the mixed-design approach adopted by this study. In this regard, the first phase of data collection exercise was in effect, adopting a cross-sectional design, and therefore taking on the principle that the organisation is to be treated as the unit of analysis. Hence, the approach of the interviews conducted in the first phase of the data collection was indeed exploratory in nature, aiming to understand and appreciate the likelihood of benefits and the associated capabilities arising from the implementation of regulatory driven IT systems in banking institutions in Malaysia. Cross-sectional design approach, in this regard, is usually adopted when a researcher wants to understand the variations between two or more cases, and where data collection is usually conducted at a particular point in time (Bryman, 2008).

b) Approach to Conducting Interviews

As mentioned earlier, the first phase of data collection exercise was primarily adopting an exploratory approach in order to gain insights into the broad areas of interest. This exploratory orientation was adopted because of the lack of past empirical research
Chapter 5: Data Gathering, Initial Analysis and Background

that would be able to provide a sound foundation for this study. Therefore, in order to fully explore the likelihood of potential benefits, the aim of the first data collection exercise was to obtain as many views as possible, with at least one interview to be conducted in each banking institution that the researcher was planning to access. Nonetheless, this specific approach was adopted without completely ignoring any openings that could be made available to the researcher (i.e. based on the ability to obtain more interview opportunities), in the effort to conduct deeper exploration within a specific organisation.

In most instances, the researcher was intending to access banking institutions that are considered to be the main market players, particularly in terms of their size of operations. This is done by also taking into consideration whether they are classified as local banking institutions, or locally incorporated foreign institutions operating in Malaysia. The reason for adopting the first principle can be attributed to the understanding that since large sized banking institutions will typically possess huge number of customers and high volume of daily transactions, they might have the tendency to establish regulatory IT systems in order to facilitate efficient regulatory compliance activities. Furthermore, in relation to the latter consideration, the measure was adopted with the intention of exploring the likelihood of potential differences in compliance efforts adopted by local banking institutions as compared to their foreign counterparts.

It is worth noting, at this juncture, that during the first phase of data collection exercise, the focus on any particular IT system was not determined, by the researcher, in advance of the interview. The selection and discussion on any specific IT system was in effect, left for the interviewee to freely decide. In this regard, the interviewees were asked to select any IT system in their organisation that was significantly influenced regulatory requirements. As far as possible, the interviewees were required to state upfront the name and functions of the chosen IT system, and the associated regulatory requirements that are seen to be influencing the implementation of this system. The regulatory IT system implementation in this context covers both; a dedicated regulatory system operating on its own; as well as a regulatory implementation or module residing in a business IT system. Although the
Chapter 5: Data Gathering, Initial Analysis and Background

study is more interested in the former, both categories of regulatory IT implementations were included in the scope of interview coverage during the first phase. This approach was taken as the interview was adopting a standpoint which tends to focus on exploring the likelihood of business benefits arising from regulatory IT implementations, regardless of where the effort that satisfies the requirements were actually residing.

c) Accessing the Research Participants

In relation to how access to conduct the interviews was achieved, the first contact made with any banking institution was typically carried out by initially communicating with officers from the Compliance department. This approach was adopted due to the understanding that since the research is concerned with regulatory compliance efforts, it is therefore sensible to firstly establish preliminary interviews with members of staff from this department. In addition, these initial contacts were subsequently aimed to provide further access to other relevant individuals that the researcher wanted to interview, i.e. in line with the principle of snowball sampling method adopted by the research.

For example, both the pilot interviewee and the contact person in Bank A were Compliance department personnel. Subsequent interviews with other staff in Bank A were conducted through the recommendations made by these two individuals. Furthermore, the approach to gain extended access to other staff within the organisation was repeated with new research participants that the researcher had managed to interview, i.e. by similarly asking for further recommendations to be made.

Additionally, expanded access to conduct interviews during the first phase was mostly achieved with other members of staff within the Compliance department. Nevertheless, this situation had one minor exception. In this regard, a representative

---

8 Please note that interviews with the other categories of research participants identified for this research, as mentioned in Section 4.5.1, were primarily conducted during the second phase of the interview exercise.
from the IT department in Bank A had indeed been included in the interview process, and the access to interview this particular IT person had been achieved through the recommendations made by the pilot interviewee. This IT department staff from Bank A was available to be interviewed during the first phase, and had been identified as the key person responsible to oversee the implementation of a new regulatory system within the organisation concern.

It is interesting to note that the subsequent recommendations to conduct interviews with other research participants in Bank A were not only limited to members of staff within the same organisation. In this regard, one of the research participants in Bank A had happened to be a committee member of CONG\(^9\) (i.e. the Compliance Officers Networking Group). This particular interviewee in Bank A was kind enough to share the research’s background information with other CONG committee members via email, in which had somewhat made subsequent access to other organisations easier in several occasions. In addition to the email sent out to other CONG members, the interviewee had also shared the contact details of several committee members that were deemed to be more experienced than others, and thus would probably be able to provide useful insights to the research.

In specific relation to Bank B, access to the research participants was achieved through the recommendations made by a contact person in this organisation. This contact person is in effect, a former central banker and is known personally to the researcher. For Bank B, the initial interview was not carried with any staff in the Compliance department. Rather, it was conducted with an individual in the organisation whom it is said to be well versed with regulatory compliance implementations within the organisation. Nevertheless, the subsequent interviews conducted in Bank B during the first phase were eventually conducted with members of staff from the Compliance department.

\(^9\) CONG committee comprises of selected compliance officers from the banking institutions, as well as representatives from the regulatory authority. The committee members meet periodically to discuss matters primarily relating to regulatory compliance. Interview quotes providing background information on this committee are available in Section 8.2.2(b).
Furthermore, in addition to the recommendations made by Bank A’s CONG committee member, as well as the contact person in Bank A and B, the effort to access potential research participants were also achieved through the researcher’s own efforts to directly approach the targeted individuals via email messages and/or phone calls. Moreover, regardless of how the initial contact was made with each organisation during the first phase, in most instances prior to the actual interview appointments, the research participants will officially be contacted via email in order to provide in advance, the necessary background information and associated documentations.\(^\text{10}\) In this regard, the “Participation Information Sheet” (which contains the research’s background information); and the “Informed Consent Form” (which primarily aimed to formally document the interviewees’ voluntary participation in the research); as well as other related documents, were provided as attachments in these email messages [see Appendices II to VI].

It is also important to note at this juncture that an interview with a person from the regulatory authority (i.e. the central bank) had also been conducted during the first phase. The interview with this particular central banker was conducted in view of the comments made by various interviewees from the banking institutions, especially when AML/CFT IT implementation had been selected as the topic for the discussion. In most instances, interviewees had highlighted this person’s name as the key contact person for any matters regarding the implementation of AML/CFT efforts within their organisations. Hence, the decision to interview this well experienced individual was to primarily attain deeper understanding on the implementation of AML/CFT requirements, as well as to solicit views regarding potential business benefits that may be experienced by banking institutions.

d) Conducting the Actual Interviews

All interviews were carried out within the banking institution’s own premises, typically in a meeting room or the interviewee’s own office in order to allow for the

\(^{10}\) There were also several occasions where the information and documentations were forwarded directly to the identified interviewees, via the contact person in a particular banking institution.
conversation to be done without much interruption. Importantly, the interviews were held closer to the working environments of the research participants with the prime intention to allow immediate request to access the associated banking documents, where possible, from the interviewees. Access to supplementary research documentations is important as these documents provide alternative insights and a deeper understanding of the research context (Bowen, 2005). Ultimately, the researcher was able to gain access to a significant amount of documentations from his interviewees [see Appendix VII].

Furthermore, in every interview conducted, all research participants had agreed that their conversations be voice recorded. A digital voice recording device was used during the interview with the intention to facilitate the transcription process later on. In addition, where possible after each interview, the researcher spent some time making field notes11 (Miles and Huberman, 1994). This activity was carried out with the aim of quickly capturing the essence of the interview, and the general impression on how the interview had been conducted (Miles and Huberman, 1994). Several researchers (e.g. Hammersley and Atkinson, 1995, Parker, 2000) have suggested that unsolicited accounts of the interview, can in effect be an excellent source for revealing information or opinion, or can even be one of the most significant part of an interview.

Equally important, a brief analysis was also subsequently conducted. The purpose of this activity was to pinpoint possible key improvement strategies that can be deployed in the research data collection exercise. Indeed, several researchers (e.g. Loftland and Loftland, 1995, Miles and Huberman, 1994) have suggested that qualitative data analysis is usually conducted as an ongoing activity, and should not be left until all the interviews are completely transcribed. This particular approach allows the researcher to be aware of any emerging issues that had been highlighted by research participants, which may warrant inclusion in the list of issues that should be addressed in subsequent interviews.

---

11 The note taking will be privately done upon the completion of an interview, either manually using pen and paper, or using the voice recorder.
Chapter 5: Data Gathering, Initial Analysis and Background

e) Number of Interviews Conducted

A total of fourteen interviews were carried out in the first phase of the data collection exercise. From this total, four interviews were conducted with members of staff in Bank A. This figure comprised of three staff from the Compliance department and one from the IT department. The three members of staff from Compliance department were; the Head of Group Compliance; a sectional head who is heading the AML/CFT efforts (and also the immediate supervisor of the pilot interviewee), and; another sectional head who is overseeing the organisation’s regulatory compliance efforts. In relation to the staff from the IT department, even though this individual was not from a managerial position, the interview was deemed critical to be conducted as this person was in effect, the IT lead for Bank A’s AML/CFT IT system.\(^{12}\)

The same number of research participants interviewed in Bank A, were also interviewed at Bank B. The four interviews from Bank B were: the Head for Business Process Development (i.e. being the first interviewee in Bank B); the Head for Group Compliance; the Project Director for AML/CFT IT system (who is also from the Compliance department), and; a Director from a wholly-owned subsidiary (i.e. the contact person).

In relation to the last interviewee, the Director from Bank B’s subsidiary was interviewed arising from the appreciation that part of the organisation’s IT operations were managed by this sister company. Furthermore, this individual has frequent meetings and interactions with other senior members of staff in Bank B (including the first two interviewees mentioned earlier) to discuss various operational matters that are affecting the organisation. Importantly, this individual is also a former central banker whom had been working with the company for about two years at the time of the interview was conducted. Therefore, this person was seen as an individual that would be able to provide valuable insights arising from the experience working on both sides of the industry (i.e. as a commercial banker, as well as a central banker). The views shared by this particular interviewee can also be deemed as unique, as they

\(^{12}\) It may be reassuring to note that the immediate supervisor for this particular interviewee (i.e. the one with a managerial position) was later interviewed during the second phase of the data collection exercise.
could not be obtained from other interviewees in Bank B, or in effect, from other organisations that the researcher was able to access to.

With regard to other banking institutions, besides Bank A and B, a total of six interviews were conducted: three interviewees are classified as from local banking institutions; two from foreign institutions; and one from the regulatory authority [see Table 5-1]:

### Table 5-1: Interview List – First Phase

<table>
<thead>
<tr>
<th>Institution</th>
<th>Role</th>
<th>Interview No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank A</td>
<td>Head of AML/CFT and Compliance Strategy</td>
<td>003</td>
</tr>
<tr>
<td></td>
<td>IT Department lead for RSA2 system</td>
<td>004</td>
</tr>
<tr>
<td></td>
<td>Head of Group Compliance</td>
<td>008</td>
</tr>
<tr>
<td></td>
<td>Head of Corporate Regulatory</td>
<td>009</td>
</tr>
<tr>
<td>Bank B</td>
<td>Director for Business Process Development</td>
<td>005</td>
</tr>
<tr>
<td></td>
<td>Vice President for Consumer Bank Risk Monitoring</td>
<td>006</td>
</tr>
<tr>
<td></td>
<td>Head of Group Compliance</td>
<td>007</td>
</tr>
<tr>
<td></td>
<td>Director from Corporate Office</td>
<td>010</td>
</tr>
<tr>
<td>Other Banks (Local)</td>
<td>Head of Branch Operations</td>
<td>012</td>
</tr>
<tr>
<td></td>
<td>Head of Operations Risk and Compliance</td>
<td>014</td>
</tr>
<tr>
<td></td>
<td>Compliance Manager</td>
<td>015</td>
</tr>
<tr>
<td>Other Banks (Foreign)</td>
<td>Regional Head of Compliance and Assurance</td>
<td>011</td>
</tr>
<tr>
<td></td>
<td>Head of Compliance and Corporate Secretary</td>
<td>013</td>
</tr>
<tr>
<td>Regulatory Authority</td>
<td>Deputy Director (1) of the Central Bank</td>
<td>016</td>
</tr>
</tbody>
</table>

### 5.2.3. Second Phase Interviews

a) **Overview**

The second phase of interview exercise was conducted for a period of slightly more than two months, after a gap of about one and a half months from the date when the first data collection had ended. The decision to allow for this gap was to enable the researcher to return to the United Kingdom and conduct a series of discussions with his research supervisor, regarding the progress and future direction of the study. In addition, during this time, the researcher was able to continue with the transcription process, and conduct a preliminary analysis of the data that had been collected.
Arising from the interviews conducted in the first phase, business benefits arising from the implementation of a regulatory driven IT system have indeed been detected in one organisation, i.e. Bank A. Hence, the preliminary analysis on the data from the exploratory nature of first phase interviews had pointed towards the need to refine the focus and scope of the research further. This approach matches with the suggestions in the literature (e.g. Miles and Huberman, 1994) which have highlighted that qualitative data analysis is often iterative in nature. In this regard, there is a repetitive engagement between collection of data and the analysis being conducted. Qualitative data analysis should commence subsequent to the collection of some data, and the output of the analysis will then shape the direction in the subsequent data collection exercise.

b) Approach to Conducting Interviews

In view of the preceding considerations, it had come to a decision that the second phase of face-to-face interview exercise will need to mainly adopt an *explanatory* approach [see also Section 5.3]. This perspective is to be implemented with the intention to further appreciate and obtain deeper insights into the notion of business benefits and the associated capabilities that were being experienced (or not being encountered) by banking institutions. It was also decided that concentrating on IT systems that are being affected by a single type of regulatory requirements (i.e. pertaining to AML/CFT) would indeed be beneficial to the research. Moreover, two major local banking institutions (i.e. Bank A and B) had also been identified and selected as the detailed case study organisations.\(^{13}\) Hence, as mentioned in Chapter 4, the second phase of data collection had utilised a *comparative design* approach, arising from the decision to primarily be based on these two organisations.

Nevertheless, it may be worth noting that the focus on these selected organisations was not in any way disregarding any opportunities to conduct interviews with

---

\(^{13}\) The rationale for choosing AML/CFT requirements and adopting the individual IS perspective; as well as the motivation to focus primarily on the two detailed case study organisations will be elaborated in detail in Section 5.3.
identified staff from other institutions, as well as the regulatory authority. Even though the research was primarily pursuing an explanatory approach, it was decided that views from other organisations were also foreseen to be beneficial to the research as well. In effect, additional insights obtained from interviews conducted with other research participants besides Bank A and B had indeed been extremely useful in the effort to obtain richer understanding of the research area, as well as contextualising the findings from the detailed case study organisations.14

c) Accessing the Research Participants

As initially mentioned during the discussion regarding access in the first phase of data collection, extended and further interactions with other research participants were mainly obtained through the already established contacts within each organisation. In specific relation to Bank A and B, the requests to meet with other potential interviewees were communicated via the relevant persons that were interviewed in the first phase. In addition, the targeted individuals in these two detailed case study organisations was also extended to members of staff from the IT department, especially to those who were deemed associated with the implementation of AML/CFT IT initiatives within each organisation. Furthermore, interviews with identified staff from relevant business departments were also pursued, primarily from the departments that were likely to have the tendency to experience business benefits from AML/CFT regulatory compliance activities. Therefore, the business departments staff interviewed during the second phase were not only originated from one specific business department. Rather, they were selected from several departments that may have potentially been experiencing or likely to encounter this type of business benefits.

14 This situation can be observed from the interview quotations used in Chapter 6 to 8, which were not originated from the research participants from the two detailed case study organisations.
Chapter 5: Data Gathering, Initial Analysis and Background

d) Conducting the Actual Interviews

Overall, a similar approach to conducting face-to-face interviews utilised in the preceding data collection exercise was also adopted in the second phase. All interviews were likewise conducted in the working environment of the research participants, and every conversation had been equally voice recorded. In addition, brief note taking and quick review were also done for each interview, once it has been completed (Miles and Huberman, 1994).¹⁵

In addition to the interviews conducted with new research participants, several follow-up interviews were also carried out with individuals that were conversed with during the first phase and pilot interviews. The purpose of this type of follow-ups (which were also done via face-to-face conversations), was to draw deeper insights from the interviewees, specifically regarding the likelihood of business benefits arising from regulatory IT implementations of AML/CFT.

Further to this, several follow-up interviews were also done via phone while the researcher was still in Malaysia, typically a few days after the actual interview with the same individuals had been conducted. However, these phone conversations were typically brief in nature, and were specifically adopted in view of the anticipated challenges in obtaining further appointments to meet these interviewees again. Importantly, a short follow-up phone interview was utilised as the objective of the conversations were primarily to obtain further clarification on specific or emerging issues discovered by the researcher, or being introduced by other interviewees. Therefore, in view of the typical fleeting nature of these phone conversations, face-to-face interactions were regarded as not a sensible solution for the researcher.

The above decision was also taken into consideration arising from the time constraint faced by the researcher during the second phase, due to the efforts to arrange and conduct longer duration face-to-face interviews with other research participants. Even though face-to-face interviews would only take an hour, on average, to be

¹⁵ Due to differing circumstances, these conditions were mainly applicable to the longer duration face-to-face interviews, and not the ones conducted via phone, especially when brief follow-ups conversations were needed.
Chapter 5: Data Gathering, Initial Analysis and Background

completed, the preparatory efforts to access potential research participants would typically require more time. Usually, these are done several days or sometimes a few weeks of advance. Hence, the researcher’s main intention during the second phase was mainly devoted to and being consumed by ensuring face-to-face interviews with identified individuals were successfully conducted.

It is important to note that the principle of theoretical saturation was used by the researcher, as far as possible, to determine whether it would be necessary to conduct further interviews, in each of the detailed case organisations. Theoretical saturation in this context can be regarded as a situation when new concepts have been explored in full, and therefore no new further insights are deemed to be available (Bryman, 2008). Consequently, the motivation is not to maximise the number of interviews, but rather to be saturated with the information being sought, and thus focusing on quality, rather than quantity (Bowen, 2005, Padgett, 1998).

In addition, even though interviews conducted during the second phase were primarily concentrating on Bank A and B, it is worth noting that other interviews were also been carried out with staff from organisations beyond these detailed case studies. Specifically relating to the interviews conducted with the other banking institutions, the principle of aiming to interact with the three targeted categories of research participants (i.e. from the Compliance department, IT department, as well as relevant business departments) were generally being adhered to, whenever it was possible to do so. The details of the interviews conducted in this phase are provided in the following section.

e) Number of Interviews Conducted

During the second phase of the data collection exercise, a total of thirty one interviews were successfully conducted (i.e. inclusive of face-to-face re-interviews and follow-ups via phone). Besides Bank A and B, staff from several organisations that were successfully interviewed during this phase includes three local banking institutions, one foreign bank, as well as from the regulatory authority.
In relation to Bank A, fifteen interviews were successfully conducted. This figure includes eight re-interview sessions, conducted either via face-to-face interviews or brief phone conversations. Apart from the IT lead for Bank A’s AML/CFT IT system who holds the position of a Senior Executive (i.e. a re-interview session), all other interviewees in the second phase were of the managerial position and above, ranging from sectional heads to the head of a department. In terms of the composition of research participants; six interviews were conducted with the staff of Compliance department; four with the IT department; and five with various business departments in Bank A.

Meanwhile, five members of staff from Bank B were interviewed in the second phase, with all having either managerial or senior management positions. All sessions were new interviews conducted via face-to-face, and the composition of research participants was: one each from the Compliance as well as the IT departments; and three from various business departments in Bank B.

It is important to note that the fewer number of interviews conducted in Bank B was due to the awareness that business benefits were not readily available in this particular organisation. As will be elaborated in the detailed analysis chapters (i.e. particularly Chapters 7 and 8), potential business benefits arising from regulatory driven IT implementations were not appreciated by the interviewees in Bank B. In effect, all research participants interviewed in Bank B during the first phase had similarly shared this sentiment. Therefore, the five new interviews conducted in Bank B during the second phase were essentially aimed to obtain confirmation on the situation affecting this organisation, and thus accessing further potential interviewees were seen as not providing material difference to the research. In contrast, some form of business benefits were indeed detected in Bank A during the first phase. Therefore the numerous interviews conducted during the second phase in Bank A were principally intended to obtain deeper clarification on how and why this particular circumstance was occurring in this organisation.

In relation to other organisations, as mentioned earlier, although this phase was primarily concentrating on Bank A and B, eleven interviews with other banking
institutions (and the regulatory authority) had also been conducted. The composition of these interviews were; six interviews were from three local banking institutions (i.e. including one re-interview via face-to-face); two from a foreign institution; and three interviewees from the regulatory authority (i.e. including one follow-up interview via phone). All research participants from other organisations that were managed to be interviewed during the second phase were of the managerial position and above, ranging from sectional heads to the ones having senior management positions. Table 5-2 provides the details of interviews conducted during the second phase of data collection:

### Table 5-2: Interview List – Second Phase

<table>
<thead>
<tr>
<th>Institution</th>
<th>Role</th>
<th>Interview No</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bank A</strong></td>
<td>Head of Analytics (Group Compliance)</td>
<td>017*; 044¹; 045²; 046³</td>
</tr>
<tr>
<td></td>
<td>IT Department lead for RSA2 system</td>
<td>018*</td>
</tr>
<tr>
<td></td>
<td>Head of GCIF</td>
<td>019</td>
</tr>
<tr>
<td></td>
<td>AVP National Sales</td>
<td>023</td>
</tr>
<tr>
<td></td>
<td>Head of CRM</td>
<td>024</td>
</tr>
<tr>
<td></td>
<td>Head of National Leads</td>
<td>030; 047⁴</td>
</tr>
<tr>
<td></td>
<td>Chief Information Officer</td>
<td>031</td>
</tr>
<tr>
<td></td>
<td>Head of AML/CFT and Compliance Strategy</td>
<td>034*</td>
</tr>
<tr>
<td></td>
<td>Head of Group Compliance</td>
<td>035*</td>
</tr>
<tr>
<td></td>
<td>Head of Solution Delivery II</td>
<td>036</td>
</tr>
<tr>
<td></td>
<td>Head of Integrated Risk Management</td>
<td>037</td>
</tr>
<tr>
<td><strong>Bank B</strong></td>
<td>Director of Consumer Bank Risk Monitoring</td>
<td>025</td>
</tr>
<tr>
<td></td>
<td>Head of Retail Banking</td>
<td>039</td>
</tr>
<tr>
<td></td>
<td>AVP, IT Department</td>
<td>040</td>
</tr>
<tr>
<td></td>
<td>Head of Preferred Banking</td>
<td>041</td>
</tr>
<tr>
<td></td>
<td>Project Manager from Transformation Office</td>
<td>042</td>
</tr>
<tr>
<td><strong>Other Banks (Local)</strong></td>
<td>Head of Group Compliance</td>
<td>020</td>
</tr>
<tr>
<td></td>
<td>Head of Compliance</td>
<td>021</td>
</tr>
<tr>
<td></td>
<td>Head of Operations Risk and Compliance</td>
<td>022*</td>
</tr>
<tr>
<td></td>
<td>Executive Director</td>
<td>026</td>
</tr>
<tr>
<td></td>
<td>Chief IT Officer</td>
<td>027</td>
</tr>
<tr>
<td></td>
<td>Chief Information Officer</td>
<td>038</td>
</tr>
<tr>
<td><strong>Other Banks (Foreign)</strong></td>
<td>Compliance Manager</td>
<td>028</td>
</tr>
<tr>
<td></td>
<td>Chief Information Officer</td>
<td>029</td>
</tr>
<tr>
<td><strong>Regulatory Authority</strong></td>
<td>Manager of the Central Bank</td>
<td>032</td>
</tr>
<tr>
<td></td>
<td>Deputy Director (2) of the Central Bank</td>
<td>033</td>
</tr>
<tr>
<td></td>
<td>Deputy Director (1) of the Central Bank</td>
<td>043⁵</td>
</tr>
</tbody>
</table>

Note: *Re-interview (via face-to-face); ⁵Re-interview (via phone)
5.2.4. Supplementary Interviews

The supplementary interview exercise was conducted with the intention to obtain the latest update on business benefits that have been identified, as well as to seek clarification on several minor gaps in understanding, arising from the outcome of the data analysis. It is important to note that these supplementary interviews were only done within one organisation, i.e. Bank A. This approach was taken because business benefits had been primarily found within this bank [see Chapter 7]. Where relevant, the updated information obtained during this phase has been reflected accordingly, within the analysis [see Chapters 6 to 8].

The supplementary data collection was done entirely via long distance phone conversations. The decision to employ phone interviews was due to the time and financial constraints affecting the researcher. In this regard, Bryman (2008) had suggested that phone interviews can also be used to generate detailed and expansive replies, in a similar level of detail generally sought by qualitative investigators. However, this technique tends to be used for interviews that are of a shorter in duration, as compared to other methods of collecting research data.

In total, five interviews were conducted with four individuals in Bank A during the supplementary phase of data collection. In addition, it may also be worth noting that all the three categories of research participants identified for this research, i.e. Compliance; IT; and business departments [see Section 4.5.1] have been successfully interviewed. However, as the purpose of the interviews was mainly to obtain an update, most of the interviews were conducted with individuals that have been interviewed in the preceding phases. Table 5-3 provides the details of supplementary interviews conducted:

<table>
<thead>
<tr>
<th>Institution</th>
<th>Role</th>
<th>Interview No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank A</td>
<td>IT Department lead for RSA2 system</td>
<td>048*; 052*</td>
</tr>
<tr>
<td></td>
<td>Head of Analytics (Group Compliance)</td>
<td>049*</td>
</tr>
<tr>
<td></td>
<td>Head of National Leads</td>
<td>050*</td>
</tr>
<tr>
<td></td>
<td>Head of CRM Technology</td>
<td>051</td>
</tr>
</tbody>
</table>

Note: *Re-interview
5.3. DATA ANALYSIS

This section will continue the discussion by outlining the data analysis activities that had been conducted by this study. In this regard, this section will build upon the general approach of analysing research data, which has been previously elaborated in Section 4.5.2.

Arising from a minor obstacle experienced by the researcher during the transcription process [see Section 9.5], the data generation in the form of interview transcripts was done via manual means. In this regard, more than forty hours of recorded interview conversations had been successfully transcribed. Since the researcher had to manually conduct the transcription by himself, the experience had allowed the researcher to be closer to the data. The ability to go through the interview numerous times during the transcription process had allowed deeper understanding on the statements made by interviewees. In addition, the process had also facilitated the efforts to read and re-read the transcripts over and over again, in order to appreciate the context of the interviewees’ statements, as well as inserting initial coding and marginal remarks (Miles and Huberman, 1994, Bryman, 2008).

The data analysis activity adopted by this research can be considered as mixed strategies, combining variable-oriented and case oriented strategies (Miles and Huberman, 1994, Ragin, 1987). In this regard, the activity undertaken subsequent to the first phase was initially adopting a variable-oriented analysis strategy (Miles and Huberman, 1994). The decision to use this analysis can be attributed to the initial approach of conducting as many interviews as possible, in order to fully explore the likelihood of potential benefits [see Section 5.2.2(b)]. Therefore a thematic analysis orientation was critical to research in order to gain insights into the areas of interest, with the main aim to identify key patterns that were prevalent across cases. In this strategy, the dynamics of each case are ignored or underplayed, with the focus to appreciate the recurring themes instead (Miles and Huberman, 1994).

It is important to note at this juncture that, due to the limited time available during the gap between the first and second data collection exercises [see Section 5.2.3(a)], the initial data analysis activity was not conducted using the NVivo software, but
Chapter 5: Data Gathering, Initial Analysis and Background

instead done manually. However, it should be noted that the write-up for the preliminary analysis of RO1a and RO2a [see subsequent Section 5.4] was premised upon a more extensive examination of the interview data, conducted when the actual data analysis phase had commenced, in earnest. This approach had been taken in order to provide thorough justifications and rationalisations to the findings.

Meanwhile, the full data analysis activity initiated right after the completion of second phase adopted a case-oriented analysis strategy (Miles and Huberman, 1994, Yin, 1984). This is done by firstly adopting a within case analysis approach in order to have an in-depth study and capture the uniqueness of an individual entity (i.e. Bank A). This approach has been adopted after taking into consideration that business benefits have primarily been detected in this organisation. Once this has been achieved, the analysis moved to the cross-case analysis approach, in order to compare and contrast the underlying themes, similarities, and deficiencies that may exist with the other detailed case study organisation (i.e. Bank B).

It is important to note at this point that besides the interview data for Bank A and B that has been used in the analysis, interviews with other banking institutions, as well as the regulatory authority were also taken into consideration. In relation to the interviews not originating from the two case study organisations, they were used to provide richer understanding, as well as contextualising the findings from the detailed case studies. Furthermore, information obtained from the review of banking documents, as well as the guidelines and legislation [see Appendix VII] have also been included in the presentation of data analysis in Chapters 6 to 8.

Overall, the discovery of underlying themes was achieved using the NVivo software. Indeed, the software has assisted in facilitating a thorough, systematic, and flexible data analysis. For instance, information for a particular code was able to be stored in single location, and easily be retrieved across all sources of interview data. In addition, the software also allows relevant nodes and sub-nodes to be easily be regrouped when needed, which has made the process of identifying patterns and themes to be more dynamic and efficient. Furthermore, NVivo was also able to provide information on the frequency of codes being cited in the interviews. Although the approach of
reporting the frequency of occurrence for a specific code was not used in this study [see Section 5.5.5(b)], this feature was useful to discover key underlying themes that should be highlighted by the research. In essence, these underlying themes were identified by appreciating the occurrence of similar codes across multiple interviews.

Although the software allows annotations to be inserted, the researcher had found it quite difficult to appreciate the usage of this feature. This is because when multiple views were displayed on the screen, it reduced the amount of information that could be seen at one time. Hence, the annotations in NVivo were not used as a replacement to the various information available via the marginal remarks (Miles and Huberman, 1994), which had already been highlighted in different colour, markings and signs, and thus were more meaningful and practical to the researcher.

5.4. PRESENTATION OF INITIAL FINDINGS

This section will continue with a presentation on the key outcomes of a preliminary analysis conducted for the research, which was premised upon the data collected during the pilot and first phase. The discussion on the initial findings will only be concentrating on two research objectives that have been previously elaborated in Chapter 3, i.e. RO1a and RO2a. The initial views and interpretations from the preliminary analysis will provide the rationale to demonstrate that these research objectives should no longer be a primary focus during the subsequent phases of data collection. On the other hand, the rest of the research objectives identified in Chapter 3 (i.e. RO1b; RO2b; RO3; and RO4) will remain as the areas of interest that the research is attempting to explore. As shown in Table 3-1, these remaining research objectives will be addressed in detail in the subsequent analysis [see Chapters 6 to 8].

Besides providing the justifications for no longer focusing on RO1a and RO2a, this section will also present the underlying reasons, as to why an explanatory approach should be adopted during the second phase. In this regard, an explanatory approach has been adopted in order to provide deeper insights into the business benefits and the associated capabilities that were being found through the interview conversations.
with research participants. In addition, as can be seen later, it has also provided the motivation for the decision to focus on a single type of regulatory requirements (i.e. pertaining to AML/CFT) and therefore primarily concentrating on IT systems being impacted by these requirements. Furthermore, it has likewise led to the justifications to adopt the perspective of an individual IS initiative; as well as the motivation to focus primarily on two large sized local banking institutions that have been chosen to be the detailed case studies for the research.

The approach of conducting a preliminary analysis matches with the suggestions in the literature that highlight the iterative nature of qualitative data analysis (e.g. Miles and Huberman, 1994). In this regard, a researcher will typically start with a concept that is broadly defined, which will then be revised and refined during data collection. In addition, this iterative approach will also correspond to one of the key concepts of grounded theory adopted by the research [see Chapter 4]. In this regard, qualitative data analysis will typically be conducted at some stage of the data collection exercise, in order to guide subsequent data collection activities.

It may be important to note at this juncture that even though this preliminary analysis was based on the data collected during the pilot and first phase, there will be instances where interview quotations from the subsequent phases were used in this section as well. The reason to adopt this approach was due to the appreciation that some interviewee statements made during these subsequent phases has provided a far better explanation and insight into the matter being discussed, as compared to the ones available during the earlier phases. Nevertheless, it is essential to reiterate that the decision to deploy the aforementioned strategies during the subsequent phases has been based solely upon the analysis conducted on the initial information gathered by the research.

5.4.1. Preliminary Findings Against Research Objectives

As mentioned earlier, the discussion on the initial findings will only be focusing on two research objectives [RO1a and RO2a]. Research objective RO1a was attempting to gain insights into the overall approaches and mechanisms by which banking
institutions translate the regulators’ requirements into functional specifications for the compliance system. In other words, it aimed at understanding the efforts that are considered basic compliance activities (and therefore, avoiding regulatory penalties). Literature, in this regard, has recommended that compliance activities be efficient and effective, i.e. by reducing redundancy and minimising associated costs. This objective can be achieved by: addressing similar required IT changes and performing them simultaneously (e.g. Mayer, 2003, Wagner and Dittmar, 2006); or using common methodologies, structures and templates (e.g. Gable, 2005).

On the other hand, research objective RO2a was aiming to appreciate banking institutions’ approaches and mechanisms that possibly taking into account other influences when responding to regulators’ requirements. In this regard, RO2a was attempting to appreciate any instances where efforts were deliberately taken to implement supplementary business related activities. These business related activities incorporate optional changes or considerations in the deployment of regulatory IT implementations that can be considered to directly benefit the organisation’s business. As conceptually suggested by the literature, this aim, among others, can be achieved by intentionally combining tactical business requirements with strategic performance opportunities (Garcia, 2004). In addition, it can also be accomplished by consciously deploying dual purpose of compliance spending by incorporating optional activities (Garcia, 2004); or implementing holistic compliance processes (Volonino et al., 2004).

a) Initial Findings in Relation to RO1a

In specific relation to RO1a, outcomes from the initial analysis had revealed that the sample institutions’ standpoint when responding to regulatory requirements was not clearly pointing towards any structured or uniform compliance approaches and mechanisms. In the effort to achieve the required state and assessing the associated gaps, activities adopted by these organisations vary extensively, and tend to be on the merits of each case. Importantly, arising from the interviews, these organisations
were not seen to be utilising predetermined methodologies, structures or templates whenever they were dealing with the requirements being imposed upon them.

Although the above may not be an ideal strategy for addressing activities that are considered mandatory, there were nevertheless still a common perspective being assumed by these institutions. As mentioned earlier, organisations tend to address the requirements in an ad-hoc nature, in which the interpretations of the requirements were carried out in an activity that is comparable to the approach of conducting any organisational project. This ad-hoc project activity utilised by these organisations is understandable, and it can partly be attributed to the common understanding on the occasional nature of regulatory requirements being issued by the regulatory authorities. Therefore, a small number of core project members (or maybe even be a single employee), would usually be appointed from the Compliance department. These individuals will typically engage, through meetings and discussion sessions, with other individuals within or outside the organisation that had been identified to be beneficial to the success of the project (e.g., representatives from the IT department, Legal department, software and hardware vendor, etc.).

As a result, determining whether the efficiency or effectiveness of banking institutions’ compliance efforts had been positively influenced, or even the associated cost being successfully minimised arising from the adaptation of structured mechanisms, were no longer regarded as a feasible route for this study to address. In effect, the cost of deploying the associated activities and efforts, as well as justifications for doing so, were not a key concern to these organisations. Their primary agenda, on the other hand, was to ensure that compliance to regulatory requirements is successfully achieved. Compliance is always a priority, and the sense of urgency and the crucialness to be compliant were detected in most interviews conducted, due to the potential adverse implications for not meeting the requirements.

Interestingly, there was also lack of evidence to suggest that these institutions were addressing similar required IT changes and performing them simultaneously. This was due to the understanding that there were “no overlapping” (005; 006; 007; 008; 009; and 010) requirements that had occurred in the first place. Therefore, prospects
of value enhancements through concerted compliance efforts by addressing multiple requirements that are of similar in nature were not discovered during the initial phases. This situation can somehow be attributed to the understanding that the banking industry is being primarily regulated by a single regulatory authority, i.e. the central bank. As a result, each set of regulatory requirements issued by this regulatory authority would typically address a specific issue of concern or interest. In addition, issuance of subsequent or additional regulatory requirements, over and above to the ones that had been previously issued, was usually meant to “complement each other” (009). Therefore, requirements originating from the same regulatory authority will typically have less possibility of being overlapped.

However, Bank A’s Head of Analytics had importantly acknowledged that if similar or overlapping requirements from multiple regulatory authorities were ever to occur, it would definitely be beneficial to the organisation, arising from having the opportunity to address multiple required changes simultaneously or within a single occasion:

“Overlapping means good to us. It’s good that in the sense that we do not have to change system so much. We do once and we can fulfil both.” (001)

Nevertheless, viewing the above statements from another perspective, it may be worth noting as well that if this particular type of cost saving benefits has indeed been realised, there is a high possibility that it will only be experienced within a single occurrence. In other words, this benefit will merely be realised when the duplication in requirements had been completely addressed during the deployment of compliance activities. On the contrary, this particular situation should be contrasted with the potential benefit of continuously appreciating the information being gathered; processed; and generated; through the implementation of a regulatory driven IT solution. Hence, the latter scenario seemed to be a far more sensible direction for the research to pursue during the subsequent phases of data collection, in comparison to the potential benefit arising from the former.
b) Initial Findings in Relation to RO2a

Moving forward to the preliminary findings in relation to RO2a, it was further revealed that the sample institutions were not seen as taking into account optional considerations whenever they were required to comply with regulatory requirements. Therefore, there was little evidence to suggest that deliberate attempts to implement supplementary activities to directly benefit banking business during the deployment of regulatory driven IT implementations, were discovered during the initial phases of the interview exercises.

It may worth noting that, especially for the case of Bank A and B, their regulatory IT systems (i.e. established for AML/CFT) can be considered as off-the-shelf or ready to use systems [see also Section 5.4.4]. Nevertheless, some customisations or configurations were indeed carried out on these systems in order to suit the unique operational nature of their organisations. Still, even with this possible avenue of incorporating supplementary activities that may benefit the business (such as, creating reports or statements for business usage, etc.), there was little evidence to suggest that activities leaning in this direction had been detected during the initial phases of the interview exercises.

In effect, these organisations were seen to be typically aiming to meet the minimum regulatory requirements, in order not to be seen as going overboard or being regarded as imposing unnecessary restrictive measures to the business. As has been explained in the preceding section, ensuring successful compliance was always seen as the overriding principle. In addition, in most interviews conducted with research participants from these banking institutions, a sense of urgency and the crucialness to be compliant were continuously detected.

Furthermore, the deployment of one regulatory IT implementation (i.e. for AML/CFT) typically fell under the responsibility of the Compliance department. Therefore, it is understandable that the principal motivation to establish this system was intended to primarily address compliance objectives. Nevertheless, even if a regulatory IT implementation is to be conducted through modifications within an IT system owned by the business (e.g. the core banking system, etc.), it is sensible to anticipate that in
most instances the changes to be made will still be influenced or monitored by the same department. Thus, it may be safe to further assume that the key motivation to ensure compliance is achieved will most likely to remain or persist.

This unwavering approach to compliance can also be further reflected through the typical absence of monetary justifications for the bank’s management, during the effort to deploy regulatory driven IT implementations within the organisation. In order words, it seemed that there was an accepted practice that a business case was usually not required in the effort to allow a regulatory IT system to be established.

Therefore, appreciating the outcomes from the preliminary analysis in relation to RO2a, it was also decided that attempts to gain insights into the possibility of organisation to adopt optional considerations within a regulatory IT implementation would not be a sensible approach to be primarily pursued during the subsequent phases of data collection.

c) Overall Findings in Relation to RO1a and RO2a

As initially revealed in Section 5.2.3(a), it should be reiterated that in the initial phases of data collection, some aspects of business benefits arising from regulatory related IT deployments have indeed been detected (i.e. in Bank A). Nevertheless, as can be seen from the preceding discussions for RO1a and RO2a, the various approaches and mechanisms suggested in the literature could not be directly associated with the benefits that have been discovered in Bank A.

As a result, this situation has presented the rationale as to why an explanatory orientation (rather than to continue with the exploratory perspective) was deemed as a sensible direction for the research to adopt, during its remaining phases. An explanatory perspective is to be adopted in order to gain richer insights as to why and how business benefits have emerged, and the role of associated capabilities in achieving this end. Importantly, as the detected benefits had not arise from the suggested approach to compliance, they can safely be assumed as having materialised, primarily from possible alternative usage of compliance information being gathered; processed; and generated by regulatory driven IT implementations. In addition, as will
be explained in the sections that follow, the research focus was also in the need of refining, and thus provides the motivation to concentrate on regulatory requirements relating specifically to AML/CFT, as well as to primarily focus on the two detailed case study organisations, i.e. Bank A and B.

5.4.2. Motivation for Focusing on AML/CFT

The second discussion on the initial findings is concerning the overall motivation to focus on a specific type of regulatory requirements, i.e. pertaining to anti-money laundering and counter financing of terrorism (AML/CFT). This guiding principle was used for the subsequent data collection phases, where the research was primarily concentrating on regulatory IT implementations being impacted by these requirements.

To briefly reiterate the statements made in Section 5.2.2(b), the approach adopted during the preceding interview exercises was that there will be no particular IT system being determined by the researcher in advance. Research participants were left to freely decide on which IT system to select and discuss. As a result, due to the wide variations of regulatory requirements and IT systems being mentioned by the interviewees, there were indeed some challenges being experienced by the researcher in gaining deeper appreciation on a particular type of regulatory IT system implementation.

Fortunately however, a majority of the interviewees in the first phase (as well as the pilot interviews) had the inclination to discuss about the implementation of AML/CFT IT systems in their organisations.¹⁶ Therefore, it was decided that specific focus on this topical regulatory requirements would be a sensible direction for this study. Furthermore, the implementation of AML/CFT in Malaysia was relatively new at the time of the interview exercise, and only limited number of local banking institutions had decided to implement an AML/CFT IT system in their organisations. Indeed, in

¹⁶ It is also acknowledged that since the first contact made with any banking institution was typically with the officers from Compliance department [see Section 5.2.2(c)], most research participants will tend to select the AML/CFT IT system during the interview, as the system is typically owned by the department.
large organisations, similar to several local banking institutions, AML/CFT IT systems were usually established as dedicated IT implementations (i.e. IT systems operating on their own software and hardware establishments). Also, for organisations that have deployed their AML/CFT IT systems, the IT solutions can still be considered as fairly new as well. Therefore, this particular situation will tend to provide an inclination where matters relating to the implementation or establishment of AML/CFT IT systems would be still in the minds, or considered as being recently experienced by a majority of the research participants. Therefore, it was envisaged that discussions regarding this issue can easily be recalled by the interviewees, in a thorough and comprehensive nature.

Furthermore, it is worth noting at this juncture that AML/CFT IT systems are typically being used to gather, process and produce the required regulatory information especially relating to their customers. Importantly, this particular system mainly analyses granular customer information, which are at the level of banking transactions. As will be explained in greater detail in Sections 5.4.4(c) and 7.5.1, for AML/CFT IT systems to effectively detect abnormal activities and provide the necessary alerts, they must have the ability to continuously analyse customers’ daily transactional data that are sourced from various banking systems. These data will subsequently be contrasted or matched with various information such as the customer’s background, profile and expected behaviour. For this reason, transactional data can be considered as one of the prerequisites in any AML/CFT IT systems.

Hence, although AML/CFT IT systems are driven by regulatory requirements and not generally perceived to directly benefit banking business, the various transactional data made available for regulatory purposes may, in effect, present an opportunity for them to be utilised for business, and therefore merits to be investigated. This notion was somewhat supported by one of the interviewees in Bank A (i.e. the IT lead for the institution’s AML/CFT IT system). In this regard, the interviewee was of the opinion that IT systems that are rich in data would definitely be beneficial and considered as an asset to the organisation:
5.4.3. Justifications for Adopting an Individual IS Orientation

As mentioned in the preceding section, it was decided that the AML/CFT requirements were to be used as a basis to evaluate any potential benefits that could be experienced by banking institutions, through the establishment of regulatory IT systems. In so doing, this study can be regarded as mainly adopting an explanatory approach from the perspective of individual IS initiative (i.e. the AML/CFT IT system) as the unit of analysis during the subsequent phases of data collection.

This particular orientation can be regarded as being in contrast to the firm-level analysis utilised by many IS researchers (e.g. Krell and Matook, 2009), which was indeed being initially adopted by the study during the earlier data collection phases.\(^\)\(^{17}\) As previous research on IT value has the tendency to utilise a firm-level orientation as the unit of analysis (Chau et al., 2007), several IS researchers have suggested that this particular approach might pose incorrect or misleading results (e.g. Doherty and Terry, 2009, Barua et al., 1995, Ray et al., 2004). Therefore, it is said that conducting similar studies at a more granular, process-level outcomes as the unit of analysis (such as from the perspective of individual IS initiative) will provide a far better representation in the assessment of IT value (e.g. Doherty and Terry, 2009, Ray et al., 2005, Bhatt and Grover, 2005). Therefore, this study had concurred with this principle and had taken the perspective of individual regulatory IS initiative in an effort to determine the possibility of it being leveraged to facilitate the creation of organisational benefits.

Furthermore, by primarily concentrating on AML/CFT requirements, the research will also only be interested in focusing on the regulatory related IS initiative that has significant potential to directly benefit the business of the organisation. This particular approach can be matched with the one taken in a study conducted by

\(^{17}\) To reiterate, the initial interview phases were adopting an exploratory approach, and treating the organisation as the unit of analysis.
Chapter 5: Data Gathering, Initial Analysis and Background

Ashurst et al. (2008). In this study, the researchers have purposely focused their research on projects that were deemed successful, in the effort to discover any evidence on the adoption of benefits realisation practices. The decision to adopt this particular approach was said to ensure that their study to remain focused only on the area of benefits realisation, and therefore totally eliminating other projects that were considered not successful.

It is also worth noting that although the primary focus during the subsequent phases of data collection was mainly concentrating on AML/CFT requirements, it was also used as a base to assess the possibility of banking institutions having evaluated other regulatory requirements as well. This consideration was taken into account with the intention to find out whether other regulatory requirements, if any, were indeed being addressed simultaneously with the requirements pertaining to AML/CFT. Hence the subsequent phases of data collection exercises were also attempting to further confirm the non-feasibility (or even possible viability) of RO1a.

5.4.4. Rationale for Concentrating on Detailed Case Studies

The fourth and last discussion on the preliminary findings and initial interpretations for this research is regarding the decision to focus on the two identified detailed case study organisations, i.e. Bank A and B. As initially mentioned in Section 5.2.2 (b), it has always been the intention of the research to target banking institutions that are considered to be the main industry players. The reason for adopting this principle is due to the general understanding that large sized banking institutions will normally possess huge number of customers and high volume of daily transactions. Therefore, due to their extensive operational capacities, these organisations could potentially have a greater incentive to establish regulatory IT systems in order to facilitate efficient compliance activities.

By contrast, this principle was not deemed to be fully applicable to foreign banking institutions operating in Malaysia. During the initial phase of data collection, it was found that foreign institutions will have the tendency to have smaller retail banking operations when compared to their local counterparts. This is due to the
understanding that their market focus tend to be concentrating on a narrower and more profitable type of banking clients, and therefore will not necessarily lead to having large number of customers with high daily transactional activities. As highlighted by the CIO of Bank A, foreign institutions tend to operate in a profitable niche market, as compared to the local banks’ intention of serving the community and addressing the mass market:

“It’s a niche, they [i.e. the foreign banks] look at where the market can generate the most values. Because of the limited branches, so they have a different strategy of focusing and generating value from their market share. Whereas the local banks are very much as mass market and try to serve the community, try to compete in terms of the points of presence, the convenience and accessibility...” (031)

Furthermore, in specific relation to AML/CFT IT implementations, it was also discovered that foreign institutions will tend to leverage existing regulatory systems made available by their head offices or overseas banking entities within their group. As related by the Head of Compliance and Corporate Secretary from a foreign banking institution, the interviewee had explicitly mentioned that all IT systems implemented in this specific organisation are either group or regional based systems:

“All our systems are either group systems or regional systems. So from IT infrastructure perspectives, we do not have a local standalone system. That’s quite different from any local bank. So for example, any system we implement, they are all group systems.” (013)

On the contrary, the establishment of AML/CFT IT systems for local banking institutions are often considered as a significant regulatory effort, since their IT solutions would normally have to be established from scratch. As acknowledged by a Head of Group Compliance from a local banking institution, foreign banks have the advantage of adopting and customising IT solutions that are made available by their headquarters. This would be in contrast to local banks which would typically need to build their solutions from the beginning:
“Because multinational banks have this advantage... they all have overseas models from the parent which they can just adopt and customise. We local banks have to do it more difficult because we have to build from the ground.” (020)

Furthermore, the need for local banks to establish an AML/CFT IT system can also be seen as a costly venture due to the huge monetary investment required to build these systems. As related by another interviewee who is a Head of Branch Operations, local banks need to invest relatively more funds as compared to foreign banks in the effort to comply with the AML/CFT requirements:

“It’s not so much of [foreign banks] incurring additional cost by introducing the system here. But for us local banks, we have to spend a lot of money.” (012)

Furthermore, as briefly highlighted earlier, local banking institutions would generally have a large number of retail customers (arising from their social responsibility), and therefore would typically be experiencing higher volume of daily transactions. Hence, the deployment of AML/CFT IT systems can thus be regarded as highly critical for these organisations, especially for the main market players. This is due to the understanding that manual AML/CFT monitoring and detection mechanisms would be considered as extremely inefficient when catering for their large customer base and a high volume of transactions. Furthermore, especially in the situation when suspicious cases have been identified, a comprehensive drill down on customers’ accounts and other information that would typically be required during an investigation, may not be able to be efficiently and effectively conducted by hand.

Nevertheless, viewing the above from another perspective, since local banking institutions are literally the absolute owners of their AML/CFT IT systems, these institutions may have more flexibility and opportunity to innovatively leverage the information amassed in their compliance systems for any other motives besides meeting regulatory requirements. In addition, in view of the significant monetary investment; extensive efforts; and possible opportunity cost, the notion of leveraging from regulatory IT implementations could be more critical to local banking institutions, as compared to their foreign equivalent.
In a nutshell, moving forward to the subsequent phases of data collection, local banking institutions seemed to be a better option for the research to focus on. This is due to their tendencies to implement AML/CFT IT system from scratch arising from not having the opportunity to leverage readily available standard IT implementations, and therefore provide alternative possibilities that could directly benefit banking business. This consideration has also led to the conclusion that it would be far more sensible for the research to primarily focus on large sized banking institutions that are of similar in nature.

The above considerations have indeed provided the justifications to select Bank A and B (i.e. large sized, local banking institutions) as the detailed case studies. In addition, this decision was also due to the understanding that these organisations had implemented their own dedicated AML/CFT IT systems in aiding and enhancing monitoring and detection capabilities. This particular condition is critical for the research, as without a successful deployment of dedicated IT solutions, it is envisaged that any potential business benefits (and their associated capabilities) might not be highly effective or comprehensive. This is due to the perceived higher efficiencies that a full-fledged IT system would typically bring to an organisation.

Nevertheless, it is also important to note that the choice of selecting Bank A and B was also due to the researcher having managed to conduct interview sessions within these organisations during the previous data collection exercise. Hence, this situation might point towards to the higher likelihood of being granted further access to other intended individuals within both organisations during the subsequent phases of interviews sessions.

5.5. CONTEXTUAL BACKGROUND

This major section will provide the background information that will set the scene for all the analysis chapters in this thesis (i.e. Chapter 6 to 8). In this regard, it will commence by providing a general backdrop on the regulatory requirements pertaining to AML/CFT, followed by a discussion on the associated requirements that are specifically affecting the Malaysian banking industry. In addition, it will also
explain the key components of a typical AML/CFT IT system, as well as briefly present the associated IT systems for the two detailed case study organisations. Importantly, the overall assumption and approach in analysing the research data being utilised in the three detailed analysis chapters will likewise be presented and discussed as well. As highlighted earlier, the adopted assumptions and approaches are introduced at this point in order to allow a more specific set of information to be presented later, where relevant and necessary to do so.

5.5.1. Background of AML/CFT Regulatory Requirements

This section is broadly divided into two parts. Firstly, it will present the information relating to AML/CFT requirements from a broad and international perspectives, before secondly, narrowing down to the specific requirements that are particularly associated with the Malaysian environment and context. The reason to adopt a broad-to-narrow approach in providing the explanation can be credited to the need to firstly appreciate and understand the overall principle that have guided and influenced the implementation of AML/CFT regulatory requirements in Malaysia. This approach was adopted in order to facilitate a more detailed and clearer discussion on the relevant requirements, which will be deployed in the three analysis chapters that follows.

a) Broad International Guidance and Principles

Overall, there are several conventions issued by the United Nations and other international bodies which on the whole, can be regarded as providing high level guidance that generally promote the prevention; criminalisation; and elimination of money laundering and terrorism financing (ML/TF). However, these international treaties can be considered as macro recommendations that are primarily focusing on country-level efforts. Examples of key international conventions aimed to address the issues pertaining to AML/CFT are as follows:

- United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) (i.e. the Vienna Convention) [D001];
• *International Convention for the Suppression of the Financing of Terrorism (1999)* [D002];

• *United Nations Convention Against Transnational Organized Crime (2000)* (i.e. the Palermo Convention) [D003];

• *Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (1990)* [D004];

• *Inter-American Convention Against Terrorism (2002)* [D005].

Moving to a slightly narrower perspective, an inter-governmental policy-making body known as the Financial Action Task Force (FATF) also develops and promotes policies to fight against ML/TF activities. Importantly, FATF’s objectives additionally include generating the political motivation to establish the necessary national legislative and regulatory reforms pertaining to AML/CFT. Furthermore, it monitors member countries’ progress in implementing activities related to the prevention of ML/TF, as well as promoting the implementation of appropriate global counter measures.\(^{18}\)

However, it is important to note that recommendations issued by FATF are not considered a binding international convention. Nevertheless, many countries have committed politically to implement them. In effect, FATF’s recommendations have generally been adopted in Malaysia through a legislation on AML/CFT, as well as within the various guidelines aiming to address a similar concern. The two most important documents that contain the key recommendations made by FATF are as follows:

• *FATF 40 Recommendations (2003)* [FATF 40] [D006]– a document that provides a set of counter-measures to prevent money laundering, which includes criminalisation and enforcement, financial system regulation, and international collaboration on AML/CFT;

• *FATF IX Special Recommendations (2001)* [FATF IX SR] [D007] – a document aimed to be combined with the recommendations in FATF 40, in order to establish the

fundamental framework in detecting, preventing and suppressing terrorist financing and acts.

Proceeding further to focus specifically on the banking industry, there are several guiding principles issued by the Basel Committee on Banking Supervision (BCBS) that can be associated with the effort of combating ML/TF. BCBS in this regard, formulates broad guidelines and supervisory standards, as well as best practices for the banking industry, in order to allow adaptation by individual countries through detailed arrangements. It also provides a forum for regular cooperation pertaining to matters on banking supervision. However, BCBS itself is not an international supervisory authority, and therefore its conclusions do not carry any legal strength. Nevertheless, measures promoted by BCBS are highly regarded and widely adopted, especially by its member countries. In specific relation to AML/CFT, BCBS has indeed issued several key documents to address this issue of interest, which are as follows:

- **The Prevention of Criminal Use of the Banking System for the Purpose of Money-Laundering (1998) [D008]** – a document that provides a general statement of ethical principles that promotes the establishment of effective procedures to prevent ML/TF activities in the banking industry;
- **Customer Due Diligence for Banks (2001) [D009]** – a document that provides a KYC (Know Your Customer) framework, which can be closely related to the effort of mitigating ML/TF activities; and
- **The Joint Forum: Initiatives by the BCBS, IAIS and IOSCO to Combat Money Laundering and the Financing of Terrorism (2003) [D010]** – a document that provides a joint document issued by BCBS; the International Association of Insurance Supervisors (IAIS); and the International Organization of Securities Commissions (IOSCO), outlining the efforts taken by each sector to combat ML/FT activities, as well as among others, an overview of the common AML/CFT standards that would apply to all three sectors.

---

19 Based on the information from BCBS’s website, [http://www.bis.org/bcbs/index.htm](http://www.bis.org/bcbs/index.htm) (accessed on 1 January, 2013).
Chapter 5: Data Gathering, Initial Analysis and Background

b) Specific Domestic Influence and Driving Factors

Having acknowledged the guiding principles issued by related international bodies, it is essential to further concentrate on requirements that are particularly associated with the context of Malaysia. This section will commence by evaluating the relevant legislation on AML/CFT, which will then explain the more detailed set of guidelines that has been issued, focusing specifically on the efforts to address matters related to the banking industry.

In connection to the legislation pertaining to AML/CFT, the Anti-Money Laundering and Anti-Terrorism Financing Act (2001), came into force in Malaysia on the 15 of January, 2002 [D011]. The Act [AMLATFA] outlines the offences pertaining to money laundering; the measures to be implemented to prevent ML/TF; as well as providing for the forfeiture of properties arising from ML/TF offences.

It is imperative to reiterate at this juncture that broad guidelines and standards issued by the international bodies, mentioned in the preceding section, do not specifically carry any punishment for being non-compliant. However, with the enforcement of AMLATFA in Malaysia, hefty financial penalties are directly imposable on instances that contravene to the requirements of the Act. It is therefore necessary to appreciate that the potentially significant monetary penalties due to non-compliance to the local AML/CFT requirements can be considered as one of the key driving factors for banking institutions to always ensure compliance is successfully achieved. To better appreciate the possible adverse financial consequences arising from the contravention to Act, key examples of these financial penalties are provided below:\(^{20}\)

- A fine of not more than RM5 million; or imprisonment for a term not exceeding 5 years; or both, for engaging; attempts to engage in; or assists in money laundering [AMLATFA, section 4(1)];
- A penalty of not more than RM1 million; or imprisonment for a period not exceeding 1 year; or both, for not adhering to the policy in retention of records [AMLATFA, section 17(4)];

\(^{20}\) Since there are numerous financial penalties being enforced by AMLATFA, this section will only provide key examples that are closely related with the specific nature of banking business.
Chapter 5: Data Gathering, Initial Analysis and Background

- A fine of not more than RM1 million; or imprisonment for a term not exceeding 1 year; or both, for opening of an account in false name [AMLATFA, section 18(5)];
- A penalty of not more than RM100,000; or imprisonment for a term not exceeding 6 months; or both, for failing to take reasonable measures to ensure compliance, or for failure to comply with any agreement with the central bank to ensure compliance. In the case of a continuing offence, a further fine of not exceeding RM1,000 for each day will be imposed [AMLATFA, section 22(4)];
- A fine of not more than RM250,000 for contravention to any provisions of the Act or other regulations made under it. This penalty is to cater for cases where no fine is specifically expressed for the offence committed under the Act or even the regulations mentioned earlier [AMLATFA, section 86].

Moving forward, arising from section 83 of AMLATFA on powers to issue guidelines; circulars; or notices, a more detailed set of guiding principles has indeed been published. In this regard, the Standard Guidelines on Anti-Money Laundering and Counter Financing of Terrorism was firstly issued by the Central Bank of Malaysia in 2006, and subsequently updated in 2009 [D012]. The Standard Guidelines [STG] were intended for all reporting institutions in all types of industry under the purview of the central bank, and outlined specific requirements that must be complied under AMLATFA. In effect, the guidelines were not only in agreement with AMLATFA, but also concurring with FATF 40; and FATF IX SR as well.

In addition to STG, it needs to be mentioned that a more detailed set of guidelines have also been issued to cater for the need of a specific industry. In specific context to the banking environment, a document known as the Anti-Money Laundering and Counter Financing of Terrorism (AML/ CFT) Sectoral Guidelines 1 for Banking and Financial Institutions had also been published accordingly in 2006 (in which, was updated in 2009 as well) [D013]. The Sectoral Guidelines 1 [SCG1] was issued specifically to address the unique requirements that must be complied by banking and financial institutions to effectively combat ML/TF activities. This document was established to specifically supplement the requirements of the STG (but addressing specific industry peculiarity), and therefore both guidelines (i.e. STG and SCG1) are
meant to be read collectively. The objective of the SCG1 is to provide the minimum standards that would allow for the development of institutions’ internal AML/CFT policies, procedures and controls.

5.5.2. Key AML/CFT Requirements for the Banking Industry

Having appreciated the relevant legislation and guidelines that are being enforced in Malaysia, it is essential to further appreciate the essence of these regulatory requirements. This approach is taken in order to briefly introduce the important areas that need to be enforced, as well as to enable a more detailed set of discussions in the subsequent analysis chapters. It is therefore necessary to appreciate that the discussion in this section should not be regarded as having comprehensively incorporated all the relevant requirements that should be associated with a specific key area being presented.

In addition, since this section will only be specifically focusing on the requirements relating to the banking industry, it will therefore be first adopting the guidelines as the basis of the discussion, and only then will subsequently consider the associated requirements in AMLATFA. Furthermore, it is essential to appreciate that the discussion in this section will primarily be concentrating on the requirements that are in relation to the context of the research. Therefore, it will be focusing on aspects of the regulatory requirements where potential benefits would most likely to emerge. Moreover, in order to facilitate a more natural and comprehensible explanation, the requirements highlighted in this section will also be clustered accordingly to several key areas, and they are reflected by the following bullet points:

- The first key area can be seen as emphasising the need to ensure banking customers are *adequately and accurately identified*. In this regard, institutions are required to develop customer acceptance policy that caters for the establishment of business relationships with the customers [STG, section 4.1.1]. In addition, customer due diligence (CDD) is also to be performed in order to obtain adequate proof, and to accurately establish the identity and legal existence of any individuals wishing to commence a business relationship with the bank [STG,
section 5.1.1; AMLATFA, sections 16(2)(a) and (b)]. Furthermore, customers’ accounts are to be maintained in the name of the account holder, and not anonymous; fictitious; false or with incorrect name [AMLATFA, sections 16(1)(a) and (b), and section 18(1)];

- Secondly, there is also a need to ensure minimum information is obtained from individual customers, such as customer’s full name; NRIC (National Registration Identity Card) or passport number; permanent and correspondence addresses; date of birth; and nationality [STG, section 5.2.1]. In addition, information such as type of occupation; name of employer; nature of business or self-employment; and contact number for home, office or mobile; are also required [SCG1, section 4.2.1];

- Thirdly, institutions need to be able to conduct customer risk profiling and categorise them according to their risk levels [STG, section 4.1.1]. In this regard, the risk profiling should at minimum, consider information such as the background or profile of customer; the nature of customer’s business; customer’s origin and location of business; as well as other information that may suggest the customer is of higher risk [STG, section 4.2.1];

- Fourthly, customer information is expected to be always kept up-to-date. In this context, institutions are required to implement continuous CDD in order to ensure the currency and relevancy of information provided [STG, section 5.1.3]. Regular reviews on current customers records are necessitated, primarily when; a significant transaction is about to occur; there is a material change on how the account is managed; there is considerable change to the customer’s documentation standards; or when the information on the customer is deemed insufficient [STG, section 5.11.2]. In addition, regular review is also needed when the nature of business of the customer changes [SCG1, section 3.1.1];

- Importantly, there is also a need to continuously monitor customers’ transactional behaviours against their profiles and backgrounds, in order to ensure consistency [STG, section 4.2.2]. An on-going CDD is required to analyse the economic background; transaction purpose; or business relationship that are; uncommon or
do not have any clear economic purpose or legitimacy, particularly when involving complex and large transactions or high-risk customers [STG, section 7.1.1];

- Finally, there is a need to establish a policy regarding retention of records. In this regard, institutions are expected to keep relevant records (in particular those obtained during CDD) for a minimum of six years retention period subsequent to the completed transaction or after the termination of the business relationship with the customer [STG, section 6.1.1; AMLATFA, section 17(1)]. Moreover, records being kept should allow for the establishment of audit trail [STG, section 6.2.2; AMLATFA, section 17(2)].

In addition to the above key areas on AML/CFT, it needs to be highlighted as well about another set of requirements that can be regarded as of equal importance. Nevertheless, it is essential to appreciate at this point that this particular key area is not being emphasised by AMLATFA, but nevertheless encouraged by the guidelines. This specific area is concerning the suggestion to establish a Management Information System (MIS) for an on-going monitoring on AML/CFT, which needs to be explicitly mentioned in this section due its intimate association with the fundamental motivation of this research.

According to the guidelines, it is recommended that an MIS is to be established in order to complement the CDD effort. The MIS, in this regard, should produce timely information on a regular basis to allow for the detection of suspicious activities, which includes; multiple and large transactions; unusual transaction patterns; or transactions that exceed any internally specified thresholds [STG, section 7.2.1]. In addition, the MIS should also be part of the institution’s information system that stores accurate and up-to-date customer’s normal transaction or business profile [STG, section 7.2.2].

5.5.3. Primary Components of an AML/CFT IT System

This section will proceed to present on what can be regarded as the key components of a typical AML/CFT IT system. It may be worth noting that these system components at this juncture, as they will facilitate deeper understanding during the
discussion for the detailed analysis chapters. The components described in this section were based on the information that have been gathered from mostly professional, as well as academic sources (e.g. Money Laundering Bulletin, 2011, Oracle, 2010, Aite, 2011, Lishan and Jun, 2011). Nevertheless, it needs to be noted that the information being presented in this section should not be viewed as conclusive, as they will definitely vary according to the solutions developed or purchased by the institutions. Moreover, the presentation for these components does not imply that they need to be incorporated in the institutions' AML/CFT IT systems, as the efforts to address matters pertaining to ML/TF, in effect, do not necessarily require to be deployed through a comprehensive IT solution.21

Generally, a typical AML/CFT IT system components may contain among others, functions to verify customers documents; conduct customer due diligence; detect suspicious transactions; facilitate case management; and confirm watch-lists (Aite, 2011, Money Laundering Bulletin, 2011). In detailed, the main components of an AML/CFT IT system can also be summarised are follows:

- **Customer due diligence** (or knowing your customer) – to validate the identity of customers; to continuously verify the information being received; as well as to ensure that the information corresponds with the customer’s subsequent transactional patterns and behaviours;

- **Behaviour profiling** – to uncover past suspicious behaviour through developing profiles of customer activities, which were also used to forecast customer’s future behaviour inclinations;

- **Suspicious transactions monitoring** – to detect prohibited money laundering activities, typically done by combining analytics and rule based approach. Rule based approach is utilised to uncover patterns of money laundering behaviours, but only for the ones that are already recognised or known. Analytics approach,

---

21 Furthermore, the list of system components was not used as a benchmark to validate the comprehensiveness of banking institutions’ AML/CFT IT systems. Also, it should not be implied that business benefits can simply be obtained by incorporating all these components within an organisation’s AML/CFT IT system.
on the other hand, is used to assist in detecting unknown scenarios that may indicate money laundering;

- *Alert management* – to assist in forwarding AML/CFT alerts to the right individual for further action, which can also be extended via email or SMS;

- *Case management* – to consolidate and centrally provide all data, notes, and activities relating to an investigation conducted by the organisation. It also provides systematic recording for compliance purposes, as well as assisting regulator’s investigations;

- *Link analysis* – to sieve through organisational data repositories to uncover suspicious relationships and complex money laundering operations, typically through business relationships; data inconsistency; and inter-related transactions;

- *Watch list filtering* – to screen customers and transactions against known watch lists (such as sanctions lists, and name list of Politically Exposed Persons (PEP));

- *Fraud prevention* – to monitor fraud within the AML/CFT IT system, which can address both AML/CFT and fraud related concerns in a single system.

### 5.5.4. Background on Detailed Case Studies’ AML/CFT IT Systems

Having recognised the various requirements, as well as the typical system components for AML/CFT, the research will now be focusing specifically to present the contextual information on AML/CFT IT systems owned by the detailed case study organisations (i.e. Bank A and B). It is imperative to note at this juncture that the information being put forward by this section was based on the insights provided by the interviewees in all stages of data collection. In addition, since this section can be considered as a brief introduction to these systems, it is also essential to appreciate that detailed associated information will likewise be further revealed within the relevant discussions in the analysis Chapters 6 to 8.
Chapter 5: Data Gathering, Initial Analysis and Background

a) Bank A

In specific relation to Bank A, at the time when the face-to-face interviews were conducted, the institution was in the midst of implementing a new dedicated AML/CFT IT system known as RSA2 (i.e. Regulatory System A2), to replace a legacy regulatory system which was said to be rather inflexible. This legacy system, RSA1 (i.e. Regulatory System A1), which can also regarded as a dedicated AML/CFT system as well, had the capability to combine both ML/TF and fraud monitoring and detection functionalities within a single IT system. RSA1 went live in 2006 and therefore had been operational for about four years at the time the interviews were conducted (018; 003).

However, it was revealed that AML/CFT functionalities in the RSA1 system were rather limited. In this regard, the system processing capabilities were only based on a limited set of data relating to current and savings accounts. In addition, RSA1 could not effectively cater for the need to conduct customer risk profiling; link analysis; as well as viewing customers from an aggregated view, which were all in accordance to the requirements imposed by the regulatory authority (003). Therefore, due to the constraints of RSA1 and its nature for not being flexible or robust enough to cater for new banking products (037; 004; 008), as well as arising from the gaps highlighted in a supervisory examination by the central bank (001; 018; 003), the management of Bank A had given the endorsement to replace RSA1 with a new AML/CFT IT system.

The new RSA2 system is said to be more flexible and scalable, and would be readily available to support the analysis using more banking products. Unlike RSA1, it will not be limited to examining transactions catering for current and savings accounts only, but can be extended to other high-risk products such as; loans; credit cards; fixed deposits; auto finance; insurance; and stock broking (003; 034). In addition, RSA2 has the ability to monitor and detect fraud activities as well (001; 004; 034; 037) [D014].

RSA2 is an off-the-shelf AML/CFT IT system developed by a software vendor. Even though it is a ready-made system, RSA2 allows some form of parameterisation to be conducted. Both RSA1 and RSA2 examine daily transactional information through an overnight batch processing, and exception reports or alerts are generated to be
reviewed in the following day (004). Therefore, both IT systems can also be regarded as backend systems that utilise information gathered from various organisational business systems to be analysed by batch for regulatory purposes.

In addition, all alerts are monitored and reviewed centrally by the Intelligence Forensics team in the Compliance department located at Bank A’s head office (003). When the need arises, related departments or branches will be solicited for the necessary information, in the effort to verify the authenticity of these alerts (018). In the case when a transaction is suspected to be associated with ML/TF activities, a Suspicious Transaction Report (STR) will be raised to the regulatory authority, i.e. the central bank.

b) **Bank B**

For the case of Bank B, the institution’s dedicated AML/CFT IT system, **RSB1** (i.e. Regulatory System B1), was first established in August 2007. Therefore, the application had already been in operation for about three years at the time when the interviews were conducted. Prior to the implementation of RSB1, the ML/TF monitoring and detection efforts were done via exception reports generated from the core banking system. The associated reports, in this regard, were printed and manually reviewed on periodic basis (025). Nevertheless, in view of the high volume of daily transactions in Bank B, as well as taking into consideration the recommendation made by the central bank, the institution had decided to establish RSB1 in order to increase the efficiency of detection and better monitoring of suspicious activities (025; 006; 005).

RSB1 is also an off-the-shelf system developed by a software vendor, and likewise, contains rules or parameters that can be refined or tweaked (040; 006). Furthermore, RSB1 has an inbuilt capability to detect fraud activities as well (006; 025). Similar to the system for Bank A, RSB1 is also an off-line or a passive AML/CFT IT system. Relevant information will be processed in batches and left to run overnight, and subsequent related reports and alerts will be generated in the following day (040). Therefore, RSB1 can also be considered as a backend system that utilises information
gathered from various organisational business systems to be analysed for regulatory purposes on a batch mode.

Nevertheless, a decentralised model in monitoring and detecting suspicious ML/TF activities was adopted in Bank B. In this regard, triggered alerts will be automatically channelled to the respective branches where the account was initially opened, i.e. the respective home branches (025; 040; 006). Bank B’s branches are then responsible to report suspected transactions to the Compliance department in the head office. Bank B’s Compliance department, in this regard, will subsequently initiate a report to the regulatory authority via raising an STR, whenever the situation warrants for it to do so.

c) Detection of Suspicious Transactions

Besides appreciating the background information pertaining to the AML/CFT IT systems owned by Bank A and B, it is highly essential to further understand how suspicious ML/TF activities would generally be detected by the system. In this regard, the following discussions will present the broad principles on how this objective is to be typically achieved.

As briefly introduced in Section 5.3.2, an AML/CFT IT system mainly analyses granular customer information, which are at the level of banking transactions, in order to detect suspicious transactions. Therefore, customer transactional data (that are sourced from various banking systems), are also regarded as one of the prerequisites to ensure the effectiveness of this regulatory system. These daily financial transactions will then be matched with customers’ background information that identifies and classifies the customers. For example, a customer may be identified as a teacher; working in the capital city; having average monthly salary; with low-risk profile; etc.

Further comparison will also be made with the customers’ anticipated financial behaviours and patterns. For example, a customer will usually be expected to receive a certain amount of money on periodic basis arising monthly salary or other earnings, etc. In addition, the customer can likewise be expected to conduct financial
transactions on regular basis, such as money transfers, regular payments and purchases, that are essentially considered to be within the customer’s means. Importantly, these contributory factors will further be assessed against known financial transactional behaviours and patterns of a typical money launderers or terrorism financiers. As suggested by the guidelines on AML/CFT [D012; and D013], for example, transactional patterns that depict rapid deposits and withdrawals of funds should trigger suspicion. Similarly, significant increase of deposits without any obvious reasons; frequent requests to exchange cash to other currencies; customers with numerous accounts and pay large amount of cash in each of them; etc., should also be treated to possibly be related with illegal activities of ML/TF. Figure 5-1 presents a simplified illustration that graphically encapsulates the above aspects of information needed for an AML/CFT IT system to effectively monitor and detect suspicious transactions: 22

![Figure 5-1: AML/CFT Analysis of Transactional Information](image)

Arising from the above comparisons, any customers’ transactional activities that do not correspond with their expected behaviours or profiles, or matches known ML/TF activities will indeed be triggered. In this regard, the AML/CFT IT system will generate alerts through its exception reporting, and be identified for further review. It is may be worth noting at this juncture that the alerted transactions highlighted by AML/CFT IT systems are in effect, yet to be confirmed as suspicious. Instead, they need to be

---

22 For reasons of simplicity, only these basic factors will be discussed in this section. Nevertheless, it is acknowledged that the AML/CFT IT system can also conduct further assessments through its analytics functions to discover complex situations and unknown scenarios that may suggest ML/TF activities, such as through link analysis [see Section 5.4.3].
further reviewed and confirmed against the profiles of the affected customers (004; 006).

The assessment activity, i.e. known as the enhance CDD process, will be conducted manually (016). As mentioned earlier, any cases that remained suspicious arising from the enhanced CDD process will require reporting to the regulatory authority in the form of raising the STR. Meanwhile, any alerts that are considered untrue (i.e. no longer considered as suspicious) will not be actioned further, and thus be classified as false positives.

5.5.5. Overall Assumption and Approach in Detailed Data Analysis

This section is specifically intended to introduce the general assumption and approach adopted by the study, in analysing and presenting research data. Rather than reiterating the same line of reasoning in all the three analysis chapters, it is more sensible for the general assumption and approach to be introduced at this juncture as broad guiding principles for the research. In addition, by adopting this perspective, it will also allow a more specific set of statements to be revealed in the relevant analysis chapters, whenever it is considered useful to do so.

a) Common Assumption in Data Analysis

In the attempt to gain deeper insights into the potential business benefits and associated capabilities of regulatory IT implementations, this research has employed one key assumption during the analysis on data being gathered by the research. In this regard, banking institutions are assumed to be in a state of full compliance with all the requirements in the guidelines (and legislation) on AML/CFT. In other words, they are regarded as having satisfied all the regulatory expectations being imposed upon them. This specific assumption was based on the understanding that if an organisation is considered as only partially compliant, any business benefits and

---

23 It is important to note that the degree of organisation’s compliance to AML/CFT regulatory requirements was not ascertained, as it will significantly undermine the impression of independence that the study is aiming to project.
associated capabilities identified by this research might not be comprehensive or thorough, as well as may even not being regarded as feasible or practicable. In addition, it may indeed be sensible to assume that organisations should be fully compliant with the requirements. This understanding can be primarily attributed to the potential adverse consequences that could arise if institutions are being classified as non-compliant, and thus being further subjected to the various possible financial penalties [see Section 5.4.1(b)];

b) General Approach in Data Analysis

In relation to the overall approach being adopted in the analysis of research data, two key considerations are worth noting. Firstly, although potential benefits arising from regulatory IT implementations can be in the form of tangible, as well as intangible benefits, the research will not be interested in distinguishing them specifically from this perspective. As initially highlighted in Chapter 3 regarding the research objectives adopted by the study, only two forms of benefits were considered to be the interest of the research. The first type of benefit, i.e. compliance benefits, can be viewed as expected or anticipated outcomes, arising from organisation’s efforts to simply meet regulatory requirements. Meanwhile, the second type of benefit, i.e. supplementary benefits, are those benefits that are achieved over and above to the ones that are usually expected and anticipated, and derived from the ability to broaden the fundamental efforts of regulatory compliance. Therefore, these two benefits categorisations are not to be further differentiated, as the effort is regarded as not contributing significantly to the discussion on the areas of interest.

Secondly, the data analysis approach for this research has no intention to quantify the findings (i.e. possessing a specific interest to the perspective of displaying the frequency of occurrence). As highlighted by the literature, the approach to quantify the findings in a qualitative research may lead to the study to being inclined in reflecting the reliability and validity criteria of quantitative research (e.g. Hesse-Biber, 1995, Bryman, 2008). Indeed, when drawing conclusions from a qualitative research, numbers do tend to be ignored (Miles and Huberman, 1994). In contrast, this study
aims to provide *thick description* (Miles and Huberman, 1994, Geertz, 1973, Denzin, 1989), as well as emphasise relevance and importance of the data to the research (Matsuo et al., 2008, Lyles and Mitroff, 1980), and thus rooted in the *compromise position*, as explained in Section 4.4.2. This is to be achieved by utilising supporting interview quotes and evidence from the review of documents, that might be able to provide good and comprehensive contextual background on the findings being discussed. In this regard, Bryman (2008) has further suggested that qualitative research is more interested in depth, as opposed to the breadth of supporting arguments, as well as having more attention to what is being considered as contextual uniqueness.

### 5.6. CONCLUDING REMARKS

Generally, this chapter has provided useful insights into the actual data collection activities and findings from the preliminary analysis, as well as the contextual and associated information relating to AML/CFT. In this regard, the chapter has successfully presented the various phases of the data collection exercises that have been deployed, as well as the rationale and motivation for focusing on AML/CFT requirements arising from the outcome of the initial findings. Importantly, it has also provided the contextual background information that is aimed to essentially set the scene for a more detailed discussion in the subsequent analysis chapters.

Next, the research will be moving to the first detailed analysis chapter that is intended to examine one of the research objectives identified in the research (i.e. RO1b). The subsequent chapter, in this regard, will therefore attempt to provide insights into the anticipated compliance benefits arising from banking institutions fundamental activities to meet regulatory requirements on AML/CFT, as well as achieving the expected regulatory deliverables.
Chapter 6

Analysis of Compliance Benefits

6.1. INTRODUCTION

This chapter will continue with the discussion by presenting the first detailed analysis for the thesis. In this regard, it will attempt to deal with one of the research objectives that have been identified in Chapter 3 (i.e. RO1b). This specific research objective is aiming to appreciate the accomplishment of compliance benefits that may be experienced by banking institutions through the implementation of regulatory compliance activities.

To briefly reiterate, compliance benefits are the type of benefits that can be regarded as somewhat expected, primarily arising from organisation’s efforts to simply meet regulatory requirements. They are therefore accomplished through implementing fundamental regulatory activities, and attaining the anticipated regulatory deliverables. Hence, these types of benefits can also be seen as being straightforwardly accomplished and realised by organisations. In addition, they can likewise considered to be achieved arising from the need to avoid the associated penalties that may be imposed due to being regarded as lacking in compliance. Importantly, performing basic regulatory activities and accomplishing the intended regulatory deliverables, in this circumstance, is carried out without exploring the possibility of implementing any broader or extended activities, considerations or changes that could directly benefit banking business.

This chapter will start the discussion by highlighting the analytical approach undertaken during the analysis of compliance benefits. In addition, the discussion on the underlying information architecture that organisations may need to establish in order to allow compliance benefits to be viable, is also presented. Furthermore, this
Chapter 6: Analysis of Compliance Benefits

This chapter will also provide a brief overview on the five major categories of compliance benefits identified, before exploring each category in detail. The extensive discussion on these five main categories will collectively form the most significant and the largest portion of the chapter. Finally, the chapter is then summarised and brought to close by the concluding remarks section.

6.1.1. Analytical Approach

Although the broad analytical approach has been articulated in Section 5.4.5(b), it is important to add the following qualifiers, which explain how the approach has been applied to compliance benefits.

Overall, the compliance benefits were detected from the analysis of the interview data, primarily through the key highlights revealed by the interviewees. These benefits were identified arising from their association with organisations’ efforts to basically meet the requirements on AML/CFT, and without the implementation of extended activities, considerations or changes that could directly benefit banking business. Importantly, as initially mentioned in Chapter 3, these compliance benefits are also regarded as the resulting condition arising from the accomplishment of expected regulatory deliverables. In other words, only by attaining the expected deliverables will the situation allows for compliance benefits to possibly be experienced by the organisations. However, it is important to appreciate that any expected deliverables should not be regarded as having a one-to-one relationship with a specific compliance benefit. As also mentioned in Chapter 3, multiple expected deliverables may effectively present similar type of benefits to the organisation. Therefore, several regulatory requirements implying expected deliverables may, in effect, produce fewer instances of compliance benefits to the organisations.24

With regard to the detection of compliance benefits via the real-life perspectives of the interviewees, it is important to appreciate that, while several research participants

---

24 This statement can be appreciated through the various sections in the regulatory requirements that were being cited, as well as being regarded as the contributing factors that have influenced the realisation of a specific compliance benefit.
have indeed acknowledged and highlighted instances that can be regarded as compliance benefits, some of these benefits were unfortunately expressed in a rather general and universal manner. In effect, several interviewees were perceived to be as though they were regurgitating on what the regulatory authority are aiming for the organisations to achieve.

Nonetheless, the detected compliance benefits were also compared and contrasted with the associated regulatory requirements on AML/CFT. This structured and comprehensive document review was conducted in order to appreciate the source requirements that may have influenced these benefits to be experienced by organisations in the first place. In addition, it has also facilitated deeper understanding on the requirements and strengthens the ability to put the statements by research participants into perspective, which have been useful to address the lack of explicitness in the articulation by some interviewees. Most significantly, as will be elaborated further in Chapter 7, the exercise has also provided deeper appreciation on the discussion on supplementary benefits that can be attained by organisations, beyond fundamental or required activities of regulatory compliance.

Exploring further on the review of regulatory requirements, this critical activity involves appreciating in detail the AML/CFT requirements that are affecting banking institutions in Malaysia. As both guidelines on AML/CFT (i.e. STG and SCG1) contained explicit requirements with which organisations would need to comply (i.e. the expected deliverables), they have been utilised in this research to act as the basis for the assessment of compliance benefits at the first instance, which were subsequently substantiated by associated sections in the legislation, where available. In addition, the review of AML/CFT requirements was only concentrating on the aspects of the requirements that deal with the associated output or expected deliverables where benefits would most likely to arise. By doing so, the research had concentrated its efforts in understanding and appreciating a specific set of regulatory requirements that are regarded to be most likely to facilitate these compliance benefits.

25 Both guidelines on AML/CFT were used as the basis for the analysis due to their greater clarity on the regulatory expectations as opposed to the one in the legislation. This is due to the understanding that these guidelines were issued to address the unique circumstances and concerns of the financial industry, as opposed to a rather universal approach typically adopted by the legislation.
Therefore, in a nutshell, the presentation of benefits in this chapter was derived from the key themes detected from the analysis of interview data, as well as, the insights obtained from a comprehensive review of the associated regulatory requirements on AML/CFT.\textsuperscript{26} Furthermore, insights obtained from the review of requirements were primarily being used as a foundation to structurally present the analysis in this chapter. The approach of developing the necessary “categorisation” arising from the collection and analysis of data is in line with the perspective adopted in qualitative research, as suggested by Bryman (2008: p. 370). Miles and Huberman (1994: p. 299) have also suggested that “there are no fixed formats” when it comes to the reporting of the analysis and interpretation of qualitative data.

On a slightly different issue, it should be further stated that although compliance benefits can be regarded as expected, they could not be equated with benefits that are being deliberately designed or planned. Organisations may be seen as aiming to comply with regulatory requirements, and thus can be regarded as planning towards being compliant and achieving the expected deliverables. However, this situation does not necessarily mean that they are intentionally planning to achieve compliance benefits, through complying with these requirements. In effect, as seen in Section 5.3.1, it may not be sensible to consider compliance benefits as intentionally planned, as the motivation for regulatory compliance was instead seen to primarily avoid adverse repercussions from the regulatory authority. Therefore, it can be further assumed that the appreciation of compliance benefits may not have been fully appreciated by organisations, in their effort primarily focus on the need to attain compliance.

6.1.2. Underlying Information Architecture

This section will proceed to present the underlying architecture that is regarded as essential to enable the achievement of compliance benefits. In this regard, there are

\textsuperscript{26}It may be essential to reiterate that compliance benefits being highlighted in this chapter were derived from organisation’s accomplishment to fundamentally meet regulatory requirements. In this regard, compliance benefits were not achieved from organisations’ compliance activities that can be considered as effective or efficient in reducing the cost of compliance (i.e. similar to the discussion in Section 5.3.1(a), on the initial findings in relation to RO1a).
various requirements in the guidelines (and legislation) on AML/CFT that can be considered as making explicit consideration for providing the underlying information infrastructure to operationally facilitate regulatory compliance. Similarly, from the perspective of the research, this underlying information should also be designed and managed in a manner that will enable and assist the realisation of compliance benefits in the organisation. Even though the suggested information architecture may bring their own distinctive compliance benefits as well, for the purpose of the analysis, they will be regarded as the prerequisite or foundational conditions that will allow for other and more meaningful compliance benefits to emerge. The regulatory requirements that have made explicit recommendations with regard to the design and management of the underlying information infrastructure are as follows:

a) *Information Retention* – the requirements pertaining information retention specify the need for organisations to retain relevant customer records (primarily for those obtained during customer due diligence [CDD]) for at least six years period. The information is required to be retained following the completion of the transaction or subsequent to the termination of business relationship with the customer. However, the record retention may be extended up to the period until the records are no longer needed, especially in cases when the information is used for an ongoing investigation or a prosecution case in the court of law [STG, sections 6.1.1 and 6.1.2; AMLATFA, section 17(1)];

b) *Comprehensive Historical Information* – in similar context to the preceding requirements, the retained customer records should also allow for the establishment of audit trail, i.e. the history, circumstances and reconstruction for each transaction. At minimum, the clarity of information should include; the identity of the customer; the beneficiary or the individual performing the transaction (where relevant); the type and form of transaction (e.g. deposit or withdrawal; by cash or other instruments, respectively); and the instruction, origin and destination of fund transfers; as well as the total and currency type [STG, section 6.2.2; AMLATFA, sections 13 and 17(2)];
c) *Timely Accessibility of Historical Information* – furthermore, it is also expected that organisations to ensure that customer records being retained are kept securely and be obtainable in a timely manner, upon request [STG, section 6.2.3];

d) *Information on Terrorists* – this requirement specifies the need for organisations to establish a database of names and particulars of terrorist according to the UN Consolidated List and other recognised list of designated individuals or entities. In addition, the database should also include orders that may be issued by the Minister of Home Affairs of Malaysia under sections of 66B and 66C of AMLATFA [STG, section 9.3]. Organisations are required to ensure that this database is up-to-date, relevant and made easily accessible to relevant organisational employees for the purpose of detecting suspicious transactions [STG, section 9.4];

e) *Information Centralisation* – this requirement outlines the need to ensure the centralisation of all information collected pursuant to Part IV of legislation on AML/CFT. The information that is expected to be centralised in this requirement is in relation to the organisations’ responsibility to submit reporting to the competent authority (i.e. the Central Bank of Malaysia) [AMLATFA, section 15].

### 6.1.3. Identified Categories of Compliance Benefits

Moving forward into the discussion specifically on the detected compliance benefits, this section will provide a brief overview on the five major categories that have been identified in the analysis. These identified categories can be regarded as being strengthened by the opportunity to leverage the underlying information architecture mentioned in the preceding section. In order to facilitate clarity, as well as ease of comprehension, the compliance benefits have been clustered into five natural groupings, and they are identified as follows:

a) *Customer Verification Benefits* – which describes the compliance benefits of being able to effectively authenticate, validate, and ensure the up-to-dateness of customers’ identifying information;

b) *Customer Monitoring Benefits* – which specifies the compliance benefits of continuously monitoring customers’ financial activities and patterns due to the
need to detect instances of suspected money laundering and terrorism financing (ML/TF) incidences;

c) **Customer Categorisation Benefits** – which outlines the compliance benefits from the ability to differentiate organisational customers based on the risk profiling information that has been established due to regulatory requirements;

d) **Computerisation Benefits** – which describes the compliance benefits that arise from computerisation and automation of AML/CFT activities in the organisation;

e) **Reputational Benefits** – which outlines the overall compliance benefits that are experienced the organisation as an entity, which will be achieved through complying with all the requirements on AML/CFT.

The detailed analysis on these identified categories of benefits is provided in the following sections.27 The presentation will typically start by outlining the associated regulatory requirements in order to provide some contextual information to the issues being discussed. This is then followed by presenting the justifications for highlighting the detected compliance benefits. In addition, relevant interview quotes expressing the views, opinions and standpoints of the research participants are also provided in order to offer richer descriptions, as well as deeper and useful insights into the area of interest. Moreover, a summary table will also be provided at the end of each section. This is done in order to structurally present responses to a set of factors and questions that are aimed to provide a clear and coherent rationalisation on the identified compliance benefits.

### 6.2. CUSTOMER VERIFICATION BENEFITS

The first category of compliance benefits outlines the potential gains and advantages that organisations will achieve by effectively authenticating and validating customers’ identifying information, in order to ensure their authenticity and accuracy. In addition, this type of compliance benefits also enables organisational AML/CFT initiatives to be

---

27 Detailed assessment of compliance benefits [as well as supplementary benefits] arising from the required changes or actions motivated by AML/CFT requirements is available in Appendix VIII.
effective by ensuring the customers’ information gathered for authentication is reliable and up-to-date. Furthermore, it also provides the benefits of mitigating the risk of ML/TF activities through the ability to cease business relationship with existing and new customers that have failed to meet the criteria set by the organisation.

The compliance benefits in this category can also be considered as the first line of defence in mitigating ML/TF activities. This is primarily attributed to the effort to validate, ensure the reliability and up-to-dateness of various customers’ identifying information which are initially ascertained when establishing business relationship with the customer. This situation can further be contrasted with the monitoring of diverse customers’ daily transactional information that are continuously altered and changed, and thus be considered as a second line of defence in AML/CFT efforts, subsequent to establishing customer relationships [see Section 6.3]. The following sections present the detailed situations where this category of compliance benefits can be achieved.

6.2.1. Customer Validation

This compliance benefit transpires from the organisational ability to efficiently and effectively conduct the customer due diligence (CDD) process in order to adequately validate and authenticate its customers. This benefit can be primarily attributed to several key sections in both guidelines and legislation on AML/CFT, which are seen to have solidly emphasised the effective deployment of CDD in the organisation. The overall requirement to conduct proper validation and authentication can be seen from the following key requirements:

- Firstly, CDD is expected to be performed on customers wishing to commence business relationship with the bank. In this regard, customer’s identity and legal existence need to be accurately and adequately established and proven, and all evidences must be confirmed by reliable and independent source documents [STG, section 5.1.1; AMLATFA, sections 16(2)(a) and (b)];
• Secondly, organisations are also required to ensure that the CDD process should at minimum be able to identify and verify the customer, as well as identify the financial transaction’s beneficial ownership and control. In addition, organisations should also be able to determine the purpose and intention of the business relationship or the business transaction [STG, sections 5.1.3 and 5.6.1; AMLATFA, section 16(3)];

• Finally, the extensiveness of customers’ information required would depend on the risk of ML/TF (such as, based on the customer’s background and the situation pertaining to the transaction that could be deemed as suspicious). In addition, it will also be relying on the type or form of transaction, and whether it involves a new product or service, or utilising new technology. Furthermore, it will likewise be contingent upon the type of customers as well (i.e. either account holders or non-account holders), and which entities they represent [SCG1, section 4.1.1].

Having stated the above somewhat predominant requirements, it is worth noting that there are also numerous additional requirements in the guidelines (and legislation) addressing specific type of banking customers and transactions, which are also necessitating effective CDD processes. Hence, the requirements in these focused sections can also be seen to be further strengthening the importance of CDD in combating ML/TF related activities. The additional requirements that are underscoring the importance of this essential activity are outlined in detail in Appendix IX.

Views from the research participants provided evidence that pointed towards to the importance of validating customers’ information, and therefore providing the foundation to achieve this compliance benefit. As highlighted by the Head of Compliance and Corporate Secretary from a foreign banking institution, customer information is essential in an organisation’s AML/CFT efforts. Therefore, it can also be concluded that ensuring customers’ information is adequately validated and authenticated can likewise be considered as equally critical:

28 The latter is in relation to the individual or party who ultimately owns or controls the customer’s transaction, especially when there is any suspicion that the transaction is conducted on behalf of a beneficial owner.
“AML is all to do with customers’ information.” (013)

Furthermore, the Head of Operations Risk and Compliance from a local banking institution had similarly suggested the overall importance in understanding the customer better, and therefore further emphasised the importance to ensure customer information is equally validated and authenticated:

“I think the main thing is we understand our customer much better. Rather you’re caught in a situation that you don’t know who you’re dealing with.” (014)

Therefore, by complying with the numerous requirements on CDD, organisations would attain compliance benefit by having the opportunity to increase their ML/TF detection effectiveness. This benefit is achieved through the ability to effectively obtain the required information from customers and accurately validate and verify their identities and statuses.

Furthermore, organisations will also possess the ability to utilise the information gathered to detect suspicious activities and subsequently able to accurately identify customers when the need arises. The benefit of detecting suspicious activities and correctly identifying customers is achievable since the customers’ identifying information has already been adequately obtained and validated upon establishing business relationship, as well as throughout the business relationship with the bank. Table 6-1 provides a structured summary of the above discussion.

<table>
<thead>
<tr>
<th>Factor</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>What</td>
<td>• What is the description of the compliance benefit?</td>
<td>• Ability to effectively detect suspected ML/TF related activities by having the ability to obtain and validate customer’s identity and legal existence.</td>
</tr>
<tr>
<td>Why</td>
<td>• Why is the compliance benefit feasible?</td>
<td>• This compliance benefit is feasible as by conducting CDD to ensure the validity and accuracy of customers’ identification information, the organisation’s ability to detect suspicious customers and correctly identify the right customers, will be enhanced.</td>
</tr>
<tr>
<td>Where</td>
<td>• Where is the compliance benefit arising?</td>
<td>• The compliance benefit is detectable within the organisation’s CDD activities (i.e. in the business departments, as well as the Compliance department).</td>
</tr>
<tr>
<td>When</td>
<td>• When will the compliance benefit be realised?</td>
<td>• The compliance benefit will be realised upon the establishment and deployment of the CDD effort in the organisation.</td>
</tr>
</tbody>
</table>
6.2.2. Information Reliability

The second type of compliance benefit relating to customer verification arises from the organisations’ ability to ensure the reliability of information gathered from customers. This compliance benefit can be achieved from the requirement to conduct on-going CDD to ensure that customer records and profiles are continuously kept updated. Regular reviews of customers’ information is especially needed when a significant transaction is about to occur, or when there is a significant change on the operation of customer’s account. In addition, reassessments are also required when there is a considerable change to the customer’s documentation standards, or when it is considered that customer information is no longer adequate [STG, sections 5.1.3; 5.11.1 and 5.11.2].

The need to ensure reliability and up-to-dateness of customers’ information can be regarded as guaranteeing the efficiency and effectiveness of organisation’s ML/TF detection activities. In addition, as suggested by Bank A’s Head of GCIF, up-to-date customer information will definitely be useful for an AML/CFT investigation:

“You see, for the AML system... to me... GCIF [i.e. the customer information] is very important if that information is current, updated regularly. So whenever they want to do investigation, it’s good [i.e. useful] for them.” (019)

Bank A’s Head of Analytics had further suggested that up-to-date customers’ information can also be obtained while addressing alerts on suspected ML/TF activities. In this regard, the review of alerts could likewise be regarded as one of the

---

29 GCIF is a section in the Data Governance Operations department that is responsible for the maintenance of customer information in Bank A.
avenues to discover inconsistencies in customer information. This situation can indeed initiate accurate information to be solicited from the customer, and subsequently be updated in the organisation’s information repository. In this regard, this interviewee had cited an example of a customer whom had opened an account while being a student, but nevertheless have not taken the effort to update the associated information once he/she had proceeded to the employment stage:

“When you opened an account 15 years ago, you put there your occupation as student. But along the way, there is no incentive for you to update that information. .... but it can be seen from the transactions that you are earning let’s say, 7 to 8 thousands [Ringgit Malaysia] per month. So the moment your transactions and your profile doesn’t jive, the system will trigger for enhance due diligence. ..... That way the branches can capture latest information.” (017)

Consequently, compliance benefits can be regarded as being achieved through the enhancement of organisational AML/CFT efforts in ensuring the reliability of customer information. In addition, building from the discussions in Section 6.2.1 (i.e. concerning the ability to obtain authenticated customer information), compounding benefits may also emerge due to the ability to ensure information reliability and up-to-dateness. In other words, as organisations are already possessing vast amount of validated and authenticated customer information, the requirement to ensure it remains reliable and up-to-date will likewise benefit their AML/CFT monitoring and detection activities. Moreover, this situation will not only enhance the effectiveness in utilising gathered information to examine customers’ accounts, but also to accurately identify customers when the need arises. Table 6-2 provides a structured summary of this situation.

<table>
<thead>
<tr>
<th>Factor</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>What</td>
<td>• What is the description of the compliance benefit?</td>
<td>• Ability to effectively detect suspected ML/TF related activities by having the ability to analyse reliable and up-to-date customers’ information.</td>
</tr>
<tr>
<td>Why</td>
<td>• Why is the compliance benefit feasible?</td>
<td>• This compliance benefit is feasible as by guaranteeing reliable and up-to-date customers’ information, the organisation’s ability to detect suspicious customers and correctly identify the right customers, will be enhanced.</td>
</tr>
</tbody>
</table>
### 6.2.3. Termination of Business Relationships

This type of compliance benefit emerges from the organisation’s ability to cease customer relationships that have failed to meet the organisational criteria, arising for the CDD process discussed in Section 6.2.1. However, this compliance benefit is not directly related to the outcomes from customer verification and authentication. Rather, this type of compliance benefit is connected to the *reactive actions* that need to be made in response to the situation when customers are not satisfying the verification and authentication standards set by the organisation. In this regard, organisations are expected to terminate business relationships with *existing customers* or prevent from commencing business relationships with *new customers* that had failed to comply with the organisation’s CDD requirements [STG, section 5.1.5]. As shared by Bank A’s Head of AML/CFT and Compliance Strategy, termination of a customer relationship can be done within a certain period arising from CDD:

“So if it hits any of the names in the blacklists, then a report will be thrown to our analytics side .... then we will communicate with branch. And we actually have in our terms of account opening, to say that we have the right within 14 days to terminate the relationship should we found out that the customer is suspicious, whatever.” (003)
Similarly, as related by a CIO (Chief Information Officer) from a foreign banking institution, business relationships with customers that are found to be blacklisted will not be extended and will subsequently be terminated:

“If these are the bad ones, or these are the blacklisted ones, then don’t take more business from them, or if they are already a customer, we have to exit from them.” (029)

Arising from the above discussion, therefore, compliance benefit can be considered as being accomplished through the requirement to end customer relationship due to AML/CFT related issues. In this regard, organisation will be able to increase their AML/CFT effectiveness through the ability to correctly deal with customers that have not satisfy their CDD process. Furthermore, arising from the ability to conduct CDD to validate customer information [see Section 6.2.1], intensified benefit may also emerge due to the ability to deploy reactive actions arising from the situation explained earlier. Table 6-3 provides a structured summary of this situation.

**Table 6-3: Benefit of Terminating Business Relationship**

<table>
<thead>
<tr>
<th>Factor</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>What</td>
<td>• What is the description of the compliance benefit?</td>
<td>• Ability to effectively reduce the risk of ML/TF related activities by having the ability to cease business relationship with related customers.</td>
</tr>
<tr>
<td>Why</td>
<td>• Why is the compliance benefit feasible?</td>
<td>• This compliance benefit is feasible with the ability to terminate business relationships with existing customers (or prevent from commencing business with new customers) that had failed to comply with the CDD requirements. Therefore, the risk of dealing with potential ML/TF activities will be mitigated.</td>
</tr>
<tr>
<td>Where</td>
<td>• Where is the compliance benefit arising?</td>
<td>• The compliance benefit is detectable within the outcome of the CDD activities (i.e. in the Compliance department, and business departments), as well as the actions that need to be made in response to exceptions, if necessary.</td>
</tr>
<tr>
<td>When</td>
<td>• When will the compliance benefit be realised?</td>
<td>• The compliance benefit will be realised upon the establishment and deployment of the CDD activities within the organisation, as well as the required actions to be made in response to the outcome of the activities.</td>
</tr>
<tr>
<td>Who</td>
<td>• Who (or which party) will have access to the compliance benefit?</td>
<td>• The Compliance department in particular, and the organisation in general will be obtaining this compliance benefit.</td>
</tr>
<tr>
<td>How</td>
<td>• How will the compliance benefit be made available?</td>
<td>• The compliance benefit will be made available via the outcome of the CDD process, and the necessary responsive actions.</td>
</tr>
</tbody>
</table>
6.3. CUSTOMER MONITORING BENEFITS

The second category of compliance benefits outlines the potential gains and advantages that organisations will achieve arising from the ability to continuously monitor customers’ financial activities and patterns based upon on the need to detect ML/TF related incidences. As initially mentioned in Section 6.2, this type of compliance benefits can also be considered as the second line of defence, in view of the regular observation of customers’ daily transactional information, which is constantly changed and modified, subsequent to establishing the relationship with banking customers. The following sections present the six specific instances where this compliance benefits can be achieved due to the implementation of AML/CFT requirements.

6.3.1. Discrepancies in Financial Transactions

The first type of compliance benefit relating to customer monitoring arises from the organisational ability to efficiently and effectively examine customers’ accounts, through on-going monitoring, to detect discrepancies, unusual, or potentially suspicious financial transactions or activities.

In this regard, organisations are expected to conduct on-going CDD that aims to analyse and clarify the economic background and purpose of any transaction or business relationship. This is done especially when transactions or relationships are uncommon or does not have any clear economic purpose or legitimacy (particularly when involving complex and large transactions, or customers of higher risks). Detection on these potential discrepancies is to be done either at the point of customer contact or through analysing the customer’s transactional activities or patterns (i.e. via continual monitoring) [STG, sections 7.1.1 and 7.1.2]. In addition, organisations are also required to establish internal criteria (known as red flags) to monitor and detect unusual or potentially suspicious transactions. Transactions that correspond to the red flags criteria are to be subjected to an enhanced CDD and on-going monitoring processes [STG, section 7.3.1].
On top of the above requirements, it is also worth noting that various sections in STG and SCG1 that are pertaining to specific type of banking customers and transactions also warrant continuous monitoring to be conducted to uncover discrepancies. The requirements in these particular sections somewhat emphasise the importance of continuous monitoring in combating ML/TF related activities. For example, for non face-to-face customers, organisations are required to implement a monitoring process that can be regarded to be at the same level of effectiveness as the one for face-to-face customers (such as ensuring on-going customer monitoring to detect discrepancies in transactions) [STG, section 5.8.3]. Furthermore, in the case of wire transfers transactions, further details are to be requested, especially in a situation that appears to be inconsistent with the customer’s usual business or activity patterns [SCG1, section 4.4.7];

The need to detect potentially suspicious financial transactions or activities through on-going monitoring has been shared by several interviewees. As highlighted by the Head of Operations Risk and Compliance from a local banking institution, monitoring of transactions need to be conducted. In addition this effort should be done from the perspective of KYC (Know Your Customer), through contrasting with customer’s information that is available within the organisation:

“So it’s very clear in the guidelines that we need to monitor transactions. So monitoring transactions not by itself, it must be monitored against KYC.” (014)

In addition, Bank A’s Head of AML/CFT and Compliance Strategy had provided an example on how an alert is triggered when inconsistencies in a customer’s profile have been detected:

“When we profile the customer against the occupation, for example, let’s say if the occupation is stated as housewife… but [the customer has] been receiving about 2 million, every week, whatever… there is a consistent big amount [of funds] coming in... that would trigger an alert already, [indicating] that something is not right with that customer.” (003)
Furthermore, the need to submit reports to the regulator arising from inconsistencies detected during the on-going monitoring has been explicitly mentioned by a Deputy Director from the regulatory authority:

“While doing business with their customers, or after reviewing the customers’ profile vis-a-vis financial activities of the accounts or the customers’ activities. If the bank finds it suspicious, they are required by law to report to us [i.e. the regulatory authority].” (016)

Therefore, by complying with the associated requirements, organisations would attain compliance benefit arising from the ability to continuously and persistently monitor customer’s transactional activities or patterns to detect potential suspicious transactions. Largely owing to continual monitoring, organisations will be able to effectively discover and detect discrepancies in financial transactions or activities that do not correspond to or be consistent with customers’ economic backgrounds and business purposes, and therefore pointing towards the possibility of ML/TF incidences. Table 6-4 provides a structured summary of the above discussion.

Table 6-4: Benefit of Discovering Discrepancies in Financial Transactions

<table>
<thead>
<tr>
<th>Factor</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>What</td>
<td>• What is the description of the compliance benefit?</td>
<td>• Ability to effectively detect suspected ML/TF related activities by uncovering customers’ financial activities and patterns that do not correspond to their economic backgrounds and business purposes.</td>
</tr>
<tr>
<td>Why</td>
<td>• Why is the compliance benefit feasible?</td>
<td>• This compliance benefit is feasible as continual monitoring would facilitate the discovery of inconsistencies, unusual, or potentially suspicious financial transactions. This is done through relentless analysis of related financial transactions or activities to detect ML/TF incidences.</td>
</tr>
<tr>
<td>Where</td>
<td>• Where is the compliance benefit arising?</td>
<td>• The compliance benefit is detectable within the on-going monitoring activities in the organisation (i.e. in the Compliance department, as well as business departments).</td>
</tr>
<tr>
<td>When</td>
<td>• When will the compliance benefit be realised?</td>
<td>• The compliance benefit will be realised upon the establishment and deployment of the continuous monitoring effort in the organisation.</td>
</tr>
<tr>
<td>Who</td>
<td>• Who (or which party) will have access to the compliance benefit?</td>
<td>• The Compliance department in particular, and the organisation in general will be obtaining this compliance benefit.</td>
</tr>
<tr>
<td>How</td>
<td>• How will the compliance benefit be made available?</td>
<td>• The compliance benefit will be made available via the outcome of the continuous monitoring.</td>
</tr>
</tbody>
</table>
6.3.2. Customer Risk Profiling

The second type of compliance benefit relating to customer monitoring evolves from the requirements to conduct risk profiling, in order to identify and assess the risk of customers pertaining to ML/TF related activities [STG, section 4.1.1]. Furthermore, organisations are expected to ensure the consistency of their customers’ risk profiles by continuously monitoring customer’s transactional activity patterns to detect unreasonable differences, which should prompt for the reassessment of the profile [STG, section 4.2.2]. Moreover, in specific relation to the banking industry (as outlined in SCG1), organisations are also required to regularly review and update the risk profiles, particularly in the case where there are changes in customer’s employment or nature of business [SCG1, section 3.1.1].

The significance of detecting discrepancies in customer risk profiling information was highlighted by several interviewees. For example, Bank A’s Head of Analytics had highlighted the ability of the RSA2 system to detect discrepancies in risk profiling information by comparing against customer’s daily transactions:

“The new system make use of the… they called it risk profiling, where they take into account the customer risk, the transaction risk, the channel risk… a lot of thing. And from there they weight the risk and the score… and then only apply that to the transaction that takes place every day.” (001)

With regard to Bank B, its Vice President for Consumer Bank Risk Monitoring had also mentioned about the establishment risk profiling information based on numerous internal risk categories and classifications, in the effort to detect suspicious transactions:

“So we basically go on profiling, where we risk profile our customers. Ok, for example if you are an accountant, you’re a lawyer, so we risk profile. We risk profile the customers and we have like 13 categories, and each category we further divide that into high, medium, low [risk categorisation]. And for each of this sub-category, we actually establish thresholds, based on volume, value, and velocity.” (006)
Importantly, views from the Head of Operations Risk and Compliance from a local banking institution had somehow summarised the significance of appreciating customer’s profile. Customer risk profiling needs to be established before organisation can have the ability to detect any discrepancies in customer’s transactions:

“When you evaluate a customer, you need to know his whole profile. Because if you don’t know his whole profile, you cannot really say that the pattern is inconsistent with his income. So you have to see the whole thing.” (022)

In relation to the need to ensure customer risk profiling information is regularly updated, Bank A’s Head of AML/CFT and Compliance Strategy had provided insights into the nature of customer risk profiling information in Bank A:

“...this risk profiling, it cannot be static, it has to be robust. Because customer’s transactions may be changing every day. So it has to keep track with the changes, of the customer’s transactions or behaviour.” (003)

The dynamic nature of customers’ risk profiling in Bank A was later confirmed in one of the banking documents that the researcher was able to access to [i.e. D015]. In this particular document, where a diagrammatical overview of RSA2 was presented, the customer risk profiling information being produced by the system was shown as being a “Real-time Risk Rating.” Furthermore, the rating itself, known as Customer Effective Risk (CER), had to go through complicated calculations that takes into consideration the weighted risk score of the Customer Core Risk (CCR) and Customer Account Aggregated Risk (CAAR). In this regard, the CCR is calculated from key customer attributes like occupation, geographical location, age, length of relationship with the bank, source of wealth, country of taxation, citizenship, etc. Whereas the CAAR, on the other hand is an aggregated risk for all accounts that the customer have with the organisation.

With regard to Bank B, although it was not specifically mentioned that the customers’ risk profiling are dynamic in nature, the ratings were equally produced through a complex calculations, which indicates similar versatility in the risk profiling arising from the potential variations of the underlying factors. Through a review of Bank B’s
Chapter 6: Analysis of Compliance Benefits

document [i.e. D020] on “Risk Profiling in RSB1 System”, the customer risk rating is calculated based on three general categorisations; i.e. the customer group (i.e. high-risk individuals or entities, foreign individuals or companies, sole proprietary and partnerships, non-profit organisations, the bank’s staff, remittance customers, etc.); the product type (e.g. current account, savings accounts, fixed deposit, etc.); and scoring (high medium, low – that is based on residence, states, occupation, industry, customer segments, country, etc.)

Therefore, by complying with the requirements mentioned earlier, organisations would attain compliance benefit by being able to deploy customers’ risk profiling. Furthermore, by having the ability to actively monitor and detect dynamic changes to customer risk profile, the organisation would be able to maintain the integrity and currency of this information, as well as continuously facilitate the discovery of customers that are suspected to be associated with ML/TF. Table 6-5 provides a structured summary of the above discussion.

Table 6-5: Benefit of Monitoring Customer Risk Profiling

<table>
<thead>
<tr>
<th>Factor</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>What</td>
<td>• What is the description of the compliance benefit?</td>
<td>• Ability to effectively monitor and detect suspected ML/TF related activities by having the ability to maintain the integrity and currency of customers’ risk profiling information.</td>
</tr>
<tr>
<td>Why</td>
<td>• Why is the compliance benefit feasible?</td>
<td>• This compliance benefit is feasible as by maintaining the integrity and currency of customers’ risk profiling information, organisations would be able to monitor and detect unreasonable changes to the risk profile. This will further facilitate the discovery of customers suspected to be involved with ML/TF activities.</td>
</tr>
<tr>
<td>Where</td>
<td>• Where is the compliance benefit arising?</td>
<td>• The compliance benefit is detectable within the deployment of customer risk profiling and on-going monitoring activities by the Compliance department.</td>
</tr>
<tr>
<td>When</td>
<td>• When will the compliance benefit be realised?</td>
<td>• The compliance benefit will be realised upon the establishment and deployment of the continuous monitoring effort on customer risk profiling within the organisation.</td>
</tr>
<tr>
<td>Who</td>
<td>• Who (or which party) will have access to the compliance benefit?</td>
<td>• The Compliance department in particular, and the organisation in general will be obtaining this compliance benefit.</td>
</tr>
<tr>
<td>How</td>
<td>• How will the compliance benefit be made available?</td>
<td>• The compliance benefit will be made available via the outcome of the continuous monitoring on customer risk profiling.</td>
</tr>
</tbody>
</table>
6.3.3. Violations in Threshold Limits

The third type of compliance benefit relating to customer monitoring arises from the organisations’ ability to effectively detect and analyse breaches in threshold limits established to discover ML/TF activities. In this regard, organisations are required to perform CDD when any of their customers’ transactions have reached or exceeded a specific transactional amount [STG, section 5.1.2]. Details of the threshold level varies according to the intended purposes, i.e. for; wire transfers; Bureau de Change services; and for occasional or cash transactions (i.e. RM3,000; RM20,000; and RM50,000, respectively) [SCG1, sections 4.1.2 to 4.1.5].

However, it is important to further note that organisations are nonetheless expected to conduct CDD regardless of the amount being transacted. This is especially warranted in situations where the organisation has reasons to suspect the occurrence of ML/TF. In this regard, the CDD process is expected to be conducted on the customer (i.e. the account owner), as well as the person conducting the transaction. In addition, organisations are also required to conduct CDD when they have any doubt on the accuracy or adequacy of information previously obtained from the customer [STG, section 5.1.2; and SCG1, section 4.1.6].

The need to effectively detect and analyse breaches in threshold limits had been mentioned by several interviewees. For instance, Bank A’s Head of AML/CFT and Compliance Strategy had highlighted the organisation’s practice for its branches to further review customers’ transactions that had breached the predefined threshold levels:

“We have threshold reports, I think about 12 or 14 reports, covering all the products, and we actually generate these threshold reports to our branches, on fortnightly basis for them to go through. If they find that the account, that particular transaction is suspicious, they should do enhanced CDD on the customer, and if it’s deemed suspicious after doing that CDD, then they have to submit STR [Suspicious Transaction Report] to us, here [i.e. in the head office].” (003)
Chapter 6: Analysis of Compliance Benefits

With regard to Bank B, its Vice President for Consumer Bank Risk Monitoring had confirmed on the establishment of threshold detection mechanisms for customers’ transactions amounting to RM50,000 and above:

“Ok, in the system for example, there is a CTR requirement, Cash Transaction Report that we say to the vendor, we must report to Bank Negara [i.e. the regulatory authority] any transactions 50 thousands and above, per customer, per account, per day basis. So they actually built that requirements and establish a parameter to that.” (006)

Similar approach in monitoring violations in threshold limits is also detected in other organisations, i.e. beyond Bank A and B. As related by the Head of Group Compliance from another local banking institution, branches are being made responsible to examine threshold reports which were generated on daily basis:

“For example the branch gets reports which identify all transactions above a certain threshold every day. So if it hits X [amount of] Ringgit [Malaysia], they will have to investigate into it, look at the background of the customer.” (020)

Therefore by abiding the aforementioned requirements, organisations would attain compliance benefit by being able to effectively uncover and analyse customers’ financial transactions that have reached or exceeded the specified threshold for the specified category and type of transactions. In addition, further compliance benefit can also be achieved through the ability to detect and examine any transactions, regardless of the amount transacted, that are seen to be suspicious and questionable. Table 6-6 provides a structured summary of the above discussion.

<table>
<thead>
<tr>
<th>Factor</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>What</td>
<td>What is the description of the compliance benefit?</td>
<td>Ability to effectively monitor and detect ML/TF related activities by having the ability to monitor threshold limits set by the organisation.</td>
</tr>
<tr>
<td>Why</td>
<td>Why is the compliance benefit feasible?</td>
<td>This compliance benefit is feasible as it will increase organisations’ AML/CFT detection effectiveness through the ability to effectively detect and analyse customers’ financial transactions that have reached or exceeded the specified threshold for the specified category and type of transactions.</td>
</tr>
</tbody>
</table>
### Chapter 6: Analysis of Compliance Benefits

<table>
<thead>
<tr>
<th>Factor</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Where</td>
<td>Where is the compliance benefit arising?</td>
<td>The compliance benefit is detectable within the on-going monitoring activities in the organisation (i.e. in the Compliance department, as well as business departments).</td>
</tr>
<tr>
<td>When</td>
<td>When will the compliance benefit be realised?</td>
<td>The compliance benefit will be realised upon the establishment and deployment of continuous monitoring effort on threshold limits within the organisation.</td>
</tr>
<tr>
<td>Who</td>
<td>Who (or which party) will have access to the compliance benefit?</td>
<td>The Compliance department in particular, and the organisation in general will be obtaining this compliance benefit.</td>
</tr>
<tr>
<td>How</td>
<td>How will the compliance benefit be made available?</td>
<td>The compliance benefit will be made available via the outcome of continuous monitoring on threshold limits.</td>
</tr>
</tbody>
</table>

#### 6.3.4. Politically Related Customers

The fourth type of compliance benefit relating to customer monitoring arises when organisations are able to continuously monitor financial transactions on customers that has been classified as Foreign Politically Exposed Persons (PEPs). PEPs in this context relate to *foreign* individuals with high status public positions, such as the head of government or senior public officials. The primary reason as to why PEPs is a concern from the perspective of ML/TF is due to the possibility of manipulations of public authority and influence to financially benefit specific individuals through illegal means, which may be rampant especially in countries where corruption issues are prevalent [STG, sections 5.9.1 and 5.9.2].

In this regard, organisations are expected to continuously perform enhanced CDD throughout the business relationship with PEPs, which should include their family members and close associates, in order to mitigate the risk of dealing with ML/TF activities [STG, section 5.9.6]. In addition, accounts relating to PEPs should also be monitored to detect discrepancies in transactions or activities as compared to their profiles [SCG1, section 4.6.1].

The above regulatory expectations to continuously monitor customers that have been classified as PEPs can be regarded as unambiguous and clear, and thus would benefit organisations that meet these requirements. Nevertheless, insights into this issue had indeed been detected during the interviews due to its significance and possible
adverse implications imposed by the regulatory authority. In this regard, the Head of Operations Risk and Compliance from a local banking institution, have strengthened the importance of monitoring PEPs within the organisational AML/CFT efforts. This is due to the power and capacity of these individuals to move illegal funds internationally (and hence running the risk of tarnishing the image of the organisation that is seen to harbour such activities):

“The reason that FATF wants us to look more on the PEPs because politically exposed [persons] would normally be very powerful people. They can move a lot of money from one country to another country.” (014)

Hence, by complying with the requirements mentioned earlier, organisations would attain compliance benefit by being able to effectively ensure that the accounts of PEPs and related individuals are examined to detect discrepancies in financial transactions or activities. Table 6-7 provides a structured summary of the above discussion.

Table 6-7: Benefit of Monitoring Politically Exposed Persons

<table>
<thead>
<tr>
<th>Factor</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>What</td>
<td>• What is the description of the compliance benefit?</td>
<td>• Ability to effectively monitor and detect ML/TF related activities by having the ability to monitor financial transactions on customers that have been categorised as PEPs.</td>
</tr>
<tr>
<td>Why</td>
<td>• Why is the compliance benefit feasible?</td>
<td>• This compliance benefit is feasible as it will increase organisations’ AML/CFT detection effectiveness through the ability to effectively ensure that the accounts of PEPs and related individuals are continuously examined to detect discrepancies in financial transactions or activities in comparison to their profiles.</td>
</tr>
<tr>
<td>Where</td>
<td>• Where is the compliance benefit arising?</td>
<td>• The compliance benefit is detectable within the on-going monitoring activities in the organisation (i.e. in the Compliance department, as well as business departments).</td>
</tr>
<tr>
<td>When</td>
<td>• When will the compliance benefit be realised?</td>
<td>• The compliance benefit will be realised upon the establishment and deployment of the continuous monitoring effort on PEPs and related individuals within the organisation.</td>
</tr>
<tr>
<td>Who</td>
<td>• Who (or which party) will have access to the compliance benefit?</td>
<td>• The Compliance department in particular, and the organisation in general will be obtaining this compliance benefit.</td>
</tr>
<tr>
<td>How</td>
<td>• How will the compliance benefit be made available?</td>
<td>• The compliance benefit will be made available via the outcome of the continuous monitoring on PEPs and related individuals.</td>
</tr>
</tbody>
</table>
6.3.5. Customers from Countries Under Observation

The fifth type of compliance benefit relating to customer monitoring emerges from the organisational ability to discover and detect customers that came from countries that are considered to have deficient AML/CFT measures. In this regard, organisations are required to conduct on-going CDD and transactions monitoring to detect individuals and business entities that originated from countries that have been deemed to have insufficient AML/CFT measures by internationally recognised bodies such as FATF. In addition, detailed further enquiries are also required to determine the background and purpose of the financial transactions or business relationship intentions from this type of customers [STG, section 7.3.2].

The need to monitor and detect customers that are originated from countries under the above categorisation had been mentioned during the interviews. For example, the Head of Operations Risk and Compliance, from a local banking institution, noted that the list containing sanctioned countries is critical, in order to ascertain that source of funds does not originate from countries that have deficient AML/CFT measures:

“So that sanction list will also have to be considered when you open an account. But the sanction list is more important for funds coming in from these countries. So we also need a system to track from which country [the funds had came from].” (014)

Furthermore, Bank A’s Head of AML/CFT and Compliance Strategy had interestingly highlighted that the checking against the list of sanctioned countries (and other listings) would normally be conducted overnight, due to the anticipated operational delays if it is done immediately:

“But a bank our size and because of the long queue at the account opening counter, it is not possible for us to check the

---

30 The Office of Foreign Assets Control (OFAC) is a government department in the United States of America that maintains and publishes the list of countries; organisational entities; or individuals that are deemed to be hostile to or intimidating the security of that country.
customer against these blacklists on the spot. So what we are doing right now, we are doing overnight.” (003)

Therefore, by complying with the associated requirements, organisations would attain compliance benefit by being able to effectively monitor customers that originated from countries that have higher inclinations of being associated with activities relating to ML/TF. Table 6-8 provides a structured summary of the above discussion.

<table>
<thead>
<tr>
<th>Factor</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>What</td>
<td>• What is the description of the compliance benefit?</td>
<td>• Ability to effectively monitor and detect ML/TF related activities through the discovery of customers that originated from countries that are considered to have deficient AML/CFT measures.</td>
</tr>
<tr>
<td>Why</td>
<td>• Why is the compliance benefit feasible?</td>
<td>• This compliance benefit is feasible as it will increase organisations’ AML/CFT detection effectiveness through the ability to effectively ensure that customers from identified countries are subjected to on-going CDD and transactions monitoring. In addition, it will also require detailed enquiries on the background and purpose of transactions or business motivations from this type of customers.</td>
</tr>
<tr>
<td>Where</td>
<td>• Where is the compliance benefit arising?</td>
<td>• The compliance benefit is detectable within the on-going monitoring activities in the organisation (i.e. in the Compliance department, as well as business departments).</td>
</tr>
<tr>
<td>When</td>
<td>• When will the compliance benefit be realised?</td>
<td>• The compliance benefit will be realised upon the establishment and deployment of the continuous monitoring effort within the organisation.</td>
</tr>
<tr>
<td>Who</td>
<td>• Who (or which party) will have access to the compliance benefit?</td>
<td>• The Compliance department in particular, and the organisation in general will be obtaining this compliance benefit.</td>
</tr>
<tr>
<td>How</td>
<td>• How will the compliance benefit be made available?</td>
<td>• The compliance benefit will be made available via the outcome of the continuous monitoring.</td>
</tr>
</tbody>
</table>

### 6.3.6. Matching of Names Under Surveillance

The sixth and the final type of compliance benefit relating to customer monitoring evolves from the requirement to ensure that the name of organisation’s customers is being actively compared with the names of known money launderers or individuals associated with terrorism financing. In this regard, organisations are required to
conduct regular assessments on new or existing customers’ names against the information in the database of names under AML/CFT surveillance. Any name match should subsequently be followed by a reasonable and proper verification to confirm the identity of the suspect. In addition, the related transactions are to be rejected (for new customers) or to be halted immediately31 (for existing customers) [STG, section 9.5]. Furthermore, in specific relation to credit card holders, organisations are also expected to reasonably ensure that the names of supplementary credit card cardholders are not listed as terrorists [SCG1, section 4.11.2].

The above requirements can also be further associated with several sections in the legislation [AMLATFA, sections 16(1)(a) and (b), and section 18(1)]. These sections require organisations to ensure that customers’ accounts are maintained in the account holder’s name, and therefore not anonymous; fictitious; false or incorrect. The importance of assuring accurate customer’s name has been placed into prominence by the legislation as the requirements will further facilitate effective AML/CFT monitoring, especially through the matching process with the list of names under surveillance.

The criticality of the requirements mentioned in the guidelines had indeed been highlighted by the interviewees. As related by Bank A’s Head of AML/CFT and Compliance Strategy, the organisation would not be able to establish banking relationship with a customer whose name matches with any of the names of suspected individuals:

“We also have another control, whereby at the point of account opening, if it hits the unwelcome customer, then the system will automatically terminate, meaning we cannot open account for that customer.” (003)

In addition, the Regional Head of Compliance and Assurance from a foreign banking institution had also mentioned about the organisation’s established process of checking the names of its banking customers:

31 Please note that the requirements in this section did not explicitly specify that business relationships with existing customers are to be ended. Therefore, this section should not be regarded as possessing similar properties with compliance benefits arising from the termination of business relationships, as explained in Section 6.2.3.
Chapter 6: Analysis of Compliance Benefits

“A thorough check on the customer’s name and background and that will churn out whether it matches with any non-desirable names.... So it will be flashed out.” (011)

Therefore, by complying with the related requirements in the guidelines and legislation, organisations would attain compliance benefit through the ability to ensure that customer’s name is true and accurate. Similar benefit will also be accomplished arising from the effort to actively compare with the list of names for individuals that are known to be associated with ML/TF. Table 6-9 provides a structured summary of the above discussion.

Table 6-9: Benefit of Matching of Names Under Surveillance

<table>
<thead>
<tr>
<th>Factor</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>What</td>
<td>• What is the description of the compliance benefit?</td>
<td>• Ability to effectively monitor and detect money launderers and terrorism financiers by having the ability to compare customer’s name with the list of names under surveillance for AML/CFT.</td>
</tr>
<tr>
<td>Why</td>
<td>• Why is the compliance benefit feasible?</td>
<td>• This compliance benefit is feasible as by ensuring that customer’s name is true and accurate, and subsequently enable active comparison with the list of names that are known to be associated with ML/TF, the effectiveness of organisations’ AML/CFT efforts will be increased.</td>
</tr>
<tr>
<td>Where</td>
<td>• Where is the compliance benefit arising?</td>
<td>• The compliance benefit is detectable within the on-going monitoring activities in the organisation (i.e. within the Compliance department, as well as business departments).</td>
</tr>
<tr>
<td>When</td>
<td>• When will the compliance benefit be realised?</td>
<td>• The compliance benefit will be realised upon the establishment and deployment of the CDD and continuous monitoring efforts within the organisation.</td>
</tr>
<tr>
<td>Who</td>
<td>• Who (or which party) will have access to the compliance benefit?</td>
<td>• The Compliance department in particular, and the organisation in general will be obtaining this compliance benefit.</td>
</tr>
<tr>
<td>How</td>
<td>• How will the compliance benefit be made available?</td>
<td>• The compliance benefit will be made available via the outcome of the continuous monitoring.</td>
</tr>
</tbody>
</table>

6.4. CUSTOMER CATEGORISATION BENEFITS

The third category of compliance benefits are potential advantages that organisations will achieve from the effective monitoring and detection of ML/TF related activities, arising from the ability to differentiate organisational customers based on the risk
profiling information that has been established due to regulatory requirements. A compliance benefit in this context will arise in the form of addressing customers differently depending upon their perceived likeliness to be involved with activities pertaining to ML/TF, as will be described in the following section.

6.4.1. Differential Engagement Strategy

This type of compliance benefit evolves from the requirements to conduct risk profiling, in order to identify and assess the risk of their customers, as well as to implement reasonable measures to address different customers’ risks [STG, sections 4.1.1 and 4.1.2]. In addition, the risk profiling is expected, at minimum, to take into account, information such as the customer’s; origin and business location; background or profile; nature of business; and any other information that may indicate that the customer is of higher risk [STG, section 4.2.1].

Furthermore, customers that are considered high-risk can be regarded as for example, the ones; having high net worth; operating cash-based business; running business/activities that are considered having high ML/TF risk; or the ones that came from areas with high crime rates [STG, section 5.10.3]. This type of customers needs to be subjected to the enhanced CDD process [STG, section 5.10.1].

Therefore, by having customers’ risk profiling information, organisations would have the opportunity to deploy differential engagement strategy with their customers. For example, as highlighted by Bank A’s Head of AML/CFT and Compliance Strategy, through customer risk rating, the bank will be able to deploy extra care when dealing with customers that have been regarded as having higher risks:

“I would say that if we are able to risk rate our customer in terms of putting the customer where they are, whether they are considered low-risk, medium-risk or high-risk, then there will be better perspectives in terms of dealing with the customer. If the business knows that they are dealing with a high-risk customer, then they will be able to take necessary precautions, to be extra careful.” (003)
Chapter 6: Analysis of Compliance Benefits

Similar sentiment in dealing with customers that have a higher level of riskiness can also be detected in Bank B. The Project Manager from Transformation Office in Bank B had also mentioned about the opportunity to avoid a certain categorisation of customers arising from the customer profiles developed through the AML/CFT effort:

“...because AML tends to provide profiles of customers, over a long time period, it gives a profile of customers. So we want these data or this information, so that when we make a plan going forward, we make sure that we try to avoid these segments of customers.” (042)

Therefore, arising from the above discussions, organisations would achieve compliance benefit by having the ability to establish a customer engagement strategy that is driven by customers’ risk categorisations (which should, at minimum, be premised on the details that have been mentioned in the requirements). In this regard, organisations will have the opportunity to undertake the necessary precautions when dealing with customers that have been regarded as possessing higher tendency to ML/TF. Overall, this compliance benefit is accomplished by deploying a customer engagement strategy that place greater emphasis on a targeted group of customers, i.e. through the implementation of a more rigorous monitoring and treatment approaches on high-risk customers (and vice versa).

However, it is essential to appreciate that this type of compliance benefit partly evolves from one of the requirements that have been mentioned in Section 6.3.2. Nonetheless, the compliance benefit that has been mentioned earlier is unrelated to the one highlighted in Section 6.3.2, through the context that had been described in the preceding paragraphs. Table 6-10 provides a structured summary of the above discussion.

Table 6-10: Benefit of Implementing Differential Engagement Strategy

<table>
<thead>
<tr>
<th>Factor</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>What</td>
<td>What is the description of the compliance benefit?</td>
<td>Ability to effectively monitor and detect ML/TF related activities by having the ability to risk categorise the customers.</td>
</tr>
<tr>
<td>Why</td>
<td>Why is the compliance benefit feasible?</td>
<td>This compliance benefit is feasible as risk categorisation of customers would enable a more exhaustive monitoring to be implemented on customers that are considered risky from AML/CFT perspectives. In addition, organisations</td>
</tr>
</tbody>
</table>
Chapter 6: Analysis of Compliance Benefits

<table>
<thead>
<tr>
<th>Factor</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Where</td>
<td>• Where is the compliance benefit arising?</td>
<td>• The compliance benefit is detectable within the information repository developed for AML/CFT.</td>
</tr>
<tr>
<td>When</td>
<td>• When will the compliance benefit be realised?</td>
<td>• The compliance benefit will be realised upon the establishment of the risk profiling and categorisation information within the organisation.</td>
</tr>
<tr>
<td>Who</td>
<td>• Who (or which party) will have access to the compliance benefit?</td>
<td>• The Compliance department in particular, and the organisation in general will be having access to this compliance benefit.</td>
</tr>
<tr>
<td>How</td>
<td>• How will the compliance benefit be made available?</td>
<td>• The compliance benefit will be made available through the repository of risk profiling and categorisation information developed for AML/CFT purposes.</td>
</tr>
</tbody>
</table>

6.5. COMPUTERISATION BENEFITS

The fourth category of compliance benefits arises from the potential gains and advantages that organisations will be achieving through effective monitoring and detection of ML/TF related activities, exclusively owing to the automation of AML/CFT activities within the organisation. It is important to note that, even though the computerisation of AML/CFT efforts may somewhat be seen as another form of underlying infrastructure, it merits to be presented in its distinct categorisation due to the justifications that will be discussed in the following section.

6.5.1. Management Information System

This compliance benefit arises from the recommendations to establish a Management Information System (MIS) to complement the organisation’s CDD effort for the purpose of AML/CFT. As initially mentioned in Section 5.4.2, the MIS is expected to produce, on a regular basis, timely information that allows for the detection of suspicious activities. In addition, it is also expected to be able to store accurate and up-to-date customer’s normal transactions or business profile, as well as be part of the organisation’s overall information system [STG, sections 7.2.1 and 7.2.2].
It is worth noting at this juncture that the computerisation of AML/CFT monitoring and detection activities is considered as non-mandatory, as it is not in any way obligated by the legislation. In addition, the two sections in the guidelines mentioned in the preceding paragraph have only explicitly encouraged for the system’s implementation. Thus, they can be further interpreted as allowing organisations some implementation flexibility in order to accommodate their unique circumstances. This particular situation can be reflected through the statements made by two interviewees from the regulatory authority. The first interviewee, a Deputy Director, had explicitly mentioned about the flexibility of implementing AML/CFT IT system:

“The Act does not prescribe, the guidelines only encourage the financial institutions [to implement].” (016)

Meanwhile, another Deputy Director had provided useful insights into the option of implementing AML/CFT IT systems. According to the interviewee, the reason why the central bank has not dictated the establishment of an IT system can be attributed to the decision to allow the explicit details of AML/CFT implementation to be decided by the banking institutions themselves (i.e. based on their unique requirements and circumstances):

“There were a lot of debates on how detailed [in the guidelines that] we want the MIS to be. But we choose to leave it to the bank to decide their requirements. Because we realised that based on our discussions with them, when we were seeking for comments and so on, we realised that many of the banks actually have various legacy systems in their institutions. So instead of telling them we need to have all these automated, we leave it to them how they might want to comply with the guidelines. Because the guidelines are just saying that you need to be able to detect and monitor unusual transactions. Now, how you are going to do it, it’s up to you.” (033)

Therefore, arising from the abovementioned flexibility, the establishment of AML/CFT IT system should not be equated to the needed underlying infrastructure that must be implemented within the organisation, as per the earlier discussion in Section 6.1.2. Nevertheless, as previously mentioned in Section 5.3.4, it is acknowledged that for
large organisations to implement AML/CFT initiatives using manual means, may not be entirely feasible. As related by Bank B’s Director for Business Process Development, the huge volume of daily transactions experienced by the bank has not made it practicable for a manual AML/CFT efforts to be implemented within the organisation:

“... because the volume is so huge, our daily transactions is so huge, the patterns are so differing that we would never be able to accommodate [on manual basis].” (005)

The above sentiment is supported by Bank B’s Vice President for Consumer Bank Risk Monitoring. The interviewee had mentioned that manual monitoring is not sensible as it is deemed as limited. In addition, the decision to establish an AML/CFT IT system had also arose from the central bank examiners’ recommendations:

“It is limited as opposed to having a system, because you cannot be monitoring the transactions through reports. So that’s why we thought it’s better to have a system. And there were also recommendations from Bank Negara when they come to audit us, perhaps a system is a better way to monitor transactions.” (006)

A similar situation is also affecting Bank A. As mentioned by Bank A’s Head of Group Compliance, the nature and high volume of transactions had made it unrealistic for Bank A’s AML/CFT efforts to operate on manual basis:

“Our supervision in terms of money laundering is highly depending on system, because of our nature of operations and volume that we transact daily is voluminous.” (008)

In addition, Bank A’s IT Department lead for the RSA2 system had also provided useful insights into the importance of an AML/CFT IT system in managing huge amount of data, and producing alerts that are able to facilitate effective CDD efforts:

“The system actually helps in the sense that you have huge amount of data and you can hardly attend to each, I mean if you have reports, even you have manual reports, you can hardly attend to all these list of possible reports. With the system, how it helps is when the data are pumped, the engine will actually
analyse, slice and dice, whatever, apply the business rules, apply the risk [rating]. So at the end of the output is, you have a focused set of alerts, so that the investigators, or the branches know which one to prioritise first.” (004)

Furthermore, in a similar situation affecting Bank B, the organisation had also decided to establish its AML/CFT IT system arising from the recommendations made by the central bank’s examiners, subsequent to a review. As related by Bank A’s Head of AML/CFT and Compliance Strategy, the regulatory authority had verbally suggested that Bank A to utilise an IT system for its AML/CFT monitoring and detection efforts:

“Actually the regulator doesn’t make it compulsory, meaning in black and white that you have to have a system. But verbally, they told us, for a bank of our size, because we have about, 12, 13 million customer size. And our daily transactions are already 3 million, per day. Throughout all the channels... Yes, cannot be done manually. It cannot be eye-ball monitoring, because we have to monitor internet channel, we have to monitor ATM transactions, we have to monitor over the counter transactions, you know, mobile, the card side... So it’s just impossible for a bank of our size to not to leverage on a system.” (003)

Hence, viewing from the unique circumstances affecting the two detailed case study organisations, it can safely be regarded the not all organisations will be experiencing this compliance benefit. This is due to the general understanding that only selected organisations will be deploying AML/CFT IT systems within their environment, which will indeed be contingent upon their organisational distinctiveness.

For that reason, due to its non-mandatory nature, the compliance benefit from the implementation of MIS within the organisations should not be considered as another form of underlying infrastructure, and therefore warrant to be presented in its own unique categorisation. Most importantly, the discussions on automation and computerisation of AML/CFT activities should not be subsumed under any other benefit categorisations, as by doing so, will increase the tendency to dilute the focus and appreciation on their unique obtainable gains and advantages. In addition, the decision to move towards this direction is also due to an intimate association to the
fundamental motivation of this research, which is to gain insights into possible benefits from the implementation of regulatory driven IT systems.

Therefore, in a nutshell, the compliance benefit obtained by organisations due to the establishment of an IT system for AML/CFT purposes would be in the form of being able to utilise the system to efficiently and effectively monitor and detect activities relating to ML/TF within the organisation. In addition, having an IT system for AML/CFT would also allow organisations to constantly monitor and detect suspicious activities by providing timely information, analysis, alerts, as well as the capability to conduct in depth drill down analysis. Table 6-11 provides a structured summary of the above discussion.

Table 6-11: Benefit of Establishing Management Information System

<table>
<thead>
<tr>
<th>Factor</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>What</td>
<td>What is the description of the compliance benefit?</td>
<td>Ability to effectively and efficiently monitor and detect suspicious activities through the implementation of MIS for AML/CFT purposes.</td>
</tr>
<tr>
<td>Why</td>
<td>Why is the compliance benefit feasible?</td>
<td>This compliance benefit is feasible as IT system for AML/CFT will constantly monitor and detect suspicious activities by providing timely information, analysis, alerts, as well as the capability to conduct in depth drill down analysis.</td>
</tr>
<tr>
<td>Where</td>
<td>Where is the compliance benefit arising?</td>
<td>The compliance benefit is detectable within the IT system established for AML/CFT purposes.</td>
</tr>
<tr>
<td>When</td>
<td>When will the compliance benefit be realised?</td>
<td>The compliance benefit will be realised upon the operationalisation of the IT system for AML/CFT purposes.</td>
</tr>
<tr>
<td>Who</td>
<td>Who (or which party) will have access to the compliance benefit?</td>
<td>The Compliance department in particular, and the organisation in general will be having access to this compliance benefit.</td>
</tr>
<tr>
<td>How</td>
<td>How will the compliance benefit be made available?</td>
<td>The compliance benefit will be made available electronically through the implementation of an IT system for AML/CFT purposes.</td>
</tr>
</tbody>
</table>

6.6. REPUTATIONAL BENEFITS

The fifth and final category of compliance benefits are potential gains and advantages that organisations will attain through being considered as generally compliant with the requirements on AML/CFT. In this regard, they can be seen as the ultimate
compliance benefits that organisations will be achieving arising from the effort to mitigate ML/TF activities. These type of compliance benefits will be in contrast to the specific benefits that have been discussed in detailed prior to this section.

Hence, the compliance benefits in this particular section will be lacking in specificity as they are not referring to any particular requirements in the guidelines or legislation. Nevertheless, even though these compliance benefits are universal in nature, they should never be ignored, but instead be equally appreciated. This is due to the understanding that they can further be considered as providing the overall context to the other compliance benefits that have been highlighted in the preceding sections.

6.6.1. Effectiveness in Monitoring and Detection

The first type of organisational compliance benefit by complying with guidelines and legislation on AML/CFT can be considered as the ability to achieve effectiveness in monitoring and detecting of ML/TF related activities through adhering the prescribed measures and meeting regulatory expectations. This compliance benefit has been interpreted from the understanding on the overall objective of both guidelines on AML/CFT, i.e. STG and SCG1. The ultimate intention of these guidelines is to effectively combat the activities of ML/TF, and therefore can be predominantly accomplished through effective and efficient monitoring and detection processes established in the organisation.

6.6.2. Mitigation of Regulatory Penalties

The second type of organisational compliance benefit is related to the ability to mitigate the risk of experiencing adverse consequences from the regulatory authority due to dissatisfactory compliance with the requirements on AML/CFT, and being subjected to the imposition of financial or non-financial penalties. As related by Bank B’s Head of Preferred Banking, complying to AML/CFT requirements is considered as a non-negotiable principle that must be adopted by organisations due to the potential adverse implications from the regulatory authority:
“Yes, you have to comply. And if you get caught not doing, the consequences are severe.” (041)

Furthermore, this compliance benefit can also be viewed from the perspective of cost avoidance, i.e. the benefit that the organisation will experience from not enduring the associated cost and losses arising from ML/TF activities. A Compliance Manager from one of the local banking institutions was of the opinion that AML/CFT efforts are basically to avoid the losses that can be experienced by the organisation, when a customer has been found to be associated with ML/TF activities:

“Because it’s a cost avoidance, and it’s also to comply with certain regulated guidelines... cost to avoid all these AML cases, all these money laundering, and terrorism financing.” (015)

The same sentiment can also be seen from the statement made by Bank A’s Head of Group Compliance that had highlighted the cost of non-compliance arising from dealings with customers that are found to be involved with similar illegal activities:

“In the end you’re doing business but the customer cannot expand, being sanctioned or being freeze, their business and their funds, and we at the end at the losing end. So non-complying is actually a cost to the bank.” (008)

Therefore, as a whole, the ability to mitigate the risk of regulatory penalties due to dissatisfactory compliance with the requirements on AML/CFT can be regarded as a form of achieving compliance benefits that can be experienced by organisations.

6.6.3. Mitigation of Adverse Organisational Reputation

In similar vein to the two preceding sections, organisations would also be able to achieve compliance benefit from mitigating the risk of adverse implications on organisational reputation arising from not being linked with the prohibited activities of ML/TF. As related by Bank A’s Head of Group Compliance, organisational reputation being tarnished through non-compliant to regulatory requirements would indeed be difficult to recover:
“...the amount which will be incurred if we are not able to comply with this money laundering reporting or tracking or what not, is actually quite high. And also there is no number to equate to that prize [i.e. penalty], and reputation is not that easy to, you know, to regain back.” (008)

The above sentiment can be further supported by Bank A’s Head of AML/CFT and Compliance Strategy. The interviewee had explicitly mentioned about maintaining organisation’s reputation when asked about the possible benefits of complying with AML/CFT regulatory requirements:

“Yeah, I think more from the reputation risk. Reputation to the organisation. Because we don’t want our organisation to be associated with... that actually provides the conduit for money laundering. I think it brings positive values to the organisation.” (003)

In relation to Bank B, its Vice President for Consumer Bank Risk Monitoring had similarly emphasised the need to protect the organisation’s reputation, when asked about the justification for implementing the AML/CFT IT system:

“...and the other thing I think that we told the management is that we have to protect our reputation. We don’t want to be known as the first bank to come out with something, that oh... money laundering is playing a time in Bank B... things like that, we don’t want that.” (006)

Furthermore, Bank B’s Head of Retail Banking had also mentioned about protecting organisational reputation when asked about the interviewee’s general opinion on the compliance function:

“At the end of the day, compliance is not going to make me money. It’s not going to generate shareholders return. But it’s an important foundation to protect reputation risk. It’s a foundation that, you know, we abide to the regulation in the spirit of regulation so at the end of the day we will not going to lose our licence.” (039)

Similarly, a Head of Branch Operations from a local banking institution had also emphasised similar importance on protecting the organisation’s image and reputation:
“You’re talking about the image. If you do not comply with the authorities, your bank’s reputation will be lost. You take years to build up a reputation, but one transaction can just bring you down.” (012)

Therefore, by being able to mitigate the risk of adverse implications on the organisation’s reputation arising from not being linked with the prohibited activities of ML/TF would be another opportunity for organisations to achieve compliance benefits from AML/CFT implementations.

6.6.4. Facilitation of Overseas Operations

The final type of organisational compliance benefit is achieved through the organisational overall ability to comply with the requirements on AML/CFT and further being able to pursue overseas banking operations, such as establishing overseas branches or providing corresponding banking services. This benefit was highlighted by an interviewee from the regulatory authority when viewed from the perspective of overall implementation of AML/CFT in the banking industry. During an interview with a Deputy Director from the regulatory authority, the interviewee had clearly mentioned about the opportunity for banks to expand internationally, when asked about the challenges experienced by the banking industry in meeting the AML/CFT requirements:

“..... those that are from big banks realised that in order for them to move internationally or at regional level, they need to have this AML [IT] system and they need to have a proper AML [mitigating efforts] in place. Otherwise it would be difficult for them to have a correspondence banking relationships with other countries. It would be difficult for them to move outside Malaysia and buying assets or buying other banks in another countries or opening a branch or subsidiary in another country. So they realised that at the end of the day, these requirements are put in also for their benefit.” (016)

It is important to note at this juncture that the above benefit was not explicitly mentioned by the interviewees from the detailed case study organisations or other
banks that the researcher was able to gain access to. Nevertheless, the above opinion can also be attributed to the general appreciation where organisations that fully comply with AML/CFT requirements can also be regarded as having substantially lesser risk of abetting or being associated with ML/TF related activities. Therefore, these organisations can be considered by international banks to be as an excellent candidate for establishing overseas banking relationships.

Furthermore, from the review of the AML/CFT guidelines, organisations are indeed expected to ensure that a proper due diligence process is deployed for assessing affiliated organisations’ feasibility in engaging correspondent banking account services. In this regard, the requirements warrant for organisations to undertake adequate measures to ensure that they are not exposed to the risk of ML/TF through the accounts maintained by the corresponding organisations [SCG1, section 4.13.1]. In addition relevant information on corresponding organisations should also be obtained and examined to assess the reputation and quality of supervision [SCG1, section 4.13.2]. Therefore, by complying with these requirements, organisations would also be able to attain compliance benefit through the ability to assure the integrity of organisation’s overseas banking business by ensuring the due diligence requirements on correspondent banking account services are met.

### 6.7. CONCLUDING REMARKS

In conclusion, this chapter has presented the compliance benefits that the sample organisations had experienced from their efforts to achieve the expected deliverables of AML/CFT requirements, primarily through the implementation of an associated IT system. The analysis of compliance benefits has been critical to this research, as it has provided empirical evidence on the availability of this type of benefits from organisation’s efforts to simply, and straightforwardly meet regulatory requirements. Importantly, it has also provided the critical foundation and justification to comprehend any instances of further benefits that can be achieved by organisations, which could directly benefit banking business. An analysis of this type of benefit, known as *supplementary benefits*, will be presented in the subsequent Chapter 7.
Chapter 7
Analysis of Supplementary Benefits

7.1. INTRODUCTION

This chapter will continue with the discussion on the second detailed analysis for the thesis. In this regard, it will be addressing another research objective that has been identified in Chapter 3 (i.e. RO2b). This specific research objective is aiming to appreciate the accomplishment of supplementary benefits that directly benefit banking business arising from the decision to leverage compliance activities.

To briefly reiterate, supplementary benefits are the type of benefits that are achieved over and above to the ones that are usually expected and anticipated. These benefits arise from activities considered to be beyond simply meeting regulatory requirements, and thus seen to directly and positively impacting the business. Therefore, they can be further regarded as not being straightforwardly accomplished, and not part of the expected deliverables typically realised through complying with regulatory requirements. As initially mentioned in Section 5.3.2, supplementary benefits arising from AML/CFT efforts can be achieved from the opportunity to alternately utilise various information (especially on banking customers) that have been made available in a regulatory IT system, in order to directly benefit the business of the organisation.

This chapter will commence by highlighting the analytical approach undertaken during the analysis of supplementary benefits. In addition, a brief overview on the five main categories of supplementary benefits that have been identified will also be presented, before exploring each category in detail. The detailed discussion on the five main categories will collectively form the most significant and the largest section of the chapter. Lastly, chapter is summarised and brought to close by the concluding remarks section.
7.1.1. Analytical Approach

In similar perspective to preceding chapter, although the broad analytical approach has been articulated in Section 5.4.5(b), it is important to add the following qualifiers, which explain how the approach has been applied to supplementary benefits.

Overall, this chapter will follow a similar approach adopted in Chapter 6. Therefore, the supplementary benefits that will be presented in this chapter have been detected from the analysis of the interview data, as well as through the appreciation on the associated regulatory requirements. Instances that can be regarded as supplementary benefits were obtained from the review of interview data, and further confirmed by the assessment of related organisational documents that have been obtained during the data collection exercises. In addition, they are also appreciated from the perspective of the source requirements that were considered relevant, through a comprehensive document review on the guidelines and legislation on AML/CFT. Nevertheless, it is important to reiterate that the detailed review was only concentrating on the aspects of the requirements that deal with the associated output or expected deliverables where benefits would most likely to arise. Therefore, the research had only intended to appreciate the specific set of requirements that are regarded to be most likely to facilitate supplementary benefits.

Importantly, the analysis of supplementary benefits had also significantly capitalised the extensive discussion on compliance benefits in Chapter 6. Insights from the identified benefits have indeed provided deeper understanding on supplementary benefits attainable by organisations. Therefore, experiencing compliance benefits can likewise be regarded as one of the prerequisite conditions for organisations to further appreciate the potential supplementary benefits that can be realised, arising from their activity to firstly meet the expected deliverables outlined by regulatory requirements.

Nevertheless, it may be worth noting that the number of supplementary benefits being presented in this chapter will slightly be smaller in terms of quantity, as compared to the number of compliance benefits that have been discussed in Chapter 6. One way of explaining this particular situation is through the standpoint that these
supplementary benefits are in effect, not the expected outcomes of a regulatory driven IT implementation within an organisation. Furthermore, it may also be regarded that not all instances of detected compliance benefits in Chapter 6 will necessarily imply supplementary benefits to be experienced by organisation, due to their potential infeasibility and impracticality.

However, although the number of detected benefits is relatively smaller, it may be reassuring to note that the presentation in this chapter can be regarded as adopting much more extensive and richer explanations as compared to the preceding chapter. This condition is particularly attributed to the need to provide a comprehensive rationalisation to the detected supplementary benefits. It is also in view of the earlier understanding that they are indeed not the outcomes that would typically be expected from any compliance activities.

Figure 7.1 below presents a general overview of the nature of relationships between the identified supplementary benefits with their corresponding compliance benefits. A more detailed discussions pertaining to the relationships between these two categories of benefits are available within the corresponding presentations for the each identified supplementary benefit.32

---

32 Please note that the relationships being presented in Figure 7-1 exclude reputational compliance benefits [see Section 6.6].
7.1.2. Identified Categories of Supplementary Benefit

In order to facilitate clarity, the identified supplementary benefits have been clustered into five plausible key categories. A brief overview of the key categories of benefits, and the detailed sections that belong to each category, is provided below:

a) **Customer Information Benefits** – which describes the supplementary benefits arising from the opportunity to leverage various readily available customer information established for regulatory purposes [Sections 7.2.1, and 7.2.2];

b) **Selective Customer Benefits** – which describes the supplementary benefits arising from the opportunity to utilise the AML/CFT screening process to effectively be selective on the type of customers that the organisation wishes to accept and maintain [Section 7.3.1];

c) **Fraud Mitigation Benefits** – which describes the supplementary benefits arising from the opportunity to leverage the functionalities for fraud monitoring and detection that have been incorporated in the AML/CFT IT system [Section 7.4.1];

d) **Information Repository Benefits** – which describes the supplementary benefits arising from the opportunity to leverage regulatory IT repository established for regulatory purposes [Section 7.5.1];

e) **Event-based Information Benefits** – which describes the supplementary benefits arising from the opportunity to leverage selected event-based customer transactional alerts generated by the AML/CFT IT system [Section 7.6.1].

It may be worth noting at this juncture regarding the general sentiment from the two interviewees from the regulatory authority, in relation to the supplementary benefits that can be obtained by the organisations arising from complying with AML/CFT requirements. As can be appreciated through the opinion of a Deputy Director, organisations will not be breaching any regulatory requirements if they wish to harvest their compliance investments for business benefits, provided that all requirements have been firstly met:

“If I’m running a business, I want to be in compliant with whatever regulations that have been imposed on me. That’s not an issue. That’s a priority. But at the same time whatever benefits that I can get out of the compliance cost that
I have to incur, I will reap that benefits. I don’t see anything wrong with it, but again this is personal view.” (016)

Meanwhile, another Deputy Director had provided useful insights into the reason why the central bank was not pursuing the route where organisations were actively encouraged to leverage AML/CFT compliance efforts to benefit business. The interviewee had highlighted that the central bank was in fact more interested to know whether other available information in the organisation has been utilised to ensure that the AML/CFT monitoring and detection are effective and efficient, rather than vice versa (i.e. by ensuring that organisational AML/CFT investment or informational outputs are being leveraged to directly facilitate business benefits):

“Well to be honest, we’ve never really gone down that road, asking are they not leveraging on the AML to do something else. It’s more the other way round, are they leveraging on the existing, let’s say customer information database for AML.” (033)

As can be appreciated from the above views, there are no unwritten rules to prevent organisations from leveraging their regulatory investments to directly benefit business. Nevertheless, the opinions from the above interviewees have indeed provided positive insights and good grounding for organisations to possibly pursue this path, which have further justify the significance of this area of interest.

In this regard, the sections that follow will provide detailed and deeper analysis on the supplementary benefits that have been identified, according to the categories mentioned earlier.33 The presentation on supplementary benefits will tend to meet the following sequence of presentation. It will typically start by providing the description of the identified benefit, as well as the rationale as to why it is worth highlighting. This is followed by an explanation on the distinctiveness of a particular benefit, in comparison to the other supplementary benefits that have been discovered and being presented in the chapter. Except in cases where the benefits are considered straightforward, or have been extensively illustrated within the discussion,

33 Detailed assessment of supplementary benefits [as well as compliance benefits] arising from the required changes or actions motivated by AML/CFT requirements is available in Appendix VIII.
a practical example on how the benefit can be realised will also be provided. This is then tailed by a discussion on the associated regulatory requirements that are considered to have influenced the realisation of supplementary benefit. Finally, relevant interview quotes expressing the views, opinions and standpoints of the research participants are also presented in order to offer richer descriptions, as well as deeper and useful insights into the area of interest.

Likewise, in order to structurally present responses to a set of factors and questions aimed at clarifying the feasibility and viability of these supplementary benefits, a summary table will also be provided at the end of each section. However, specifically for the purpose of appreciating supplementary benefits, one additional question has been added in an attempt to assess the usefulness of identified benefits. This additional assessment is included in order to importantly ascertain the practicality and feasibility of the identified benefits, in contrast to other possible alternative sources that may produce similar and comparable benefits, which may exist within the organisation.

7.2. CUSTOMER INFORMATION BENEFITS

The first category of supplementary benefits outlines the business gains and advantages arising from the opportunity to leverage various readily available customer information established for regulatory purposes. The customer information in this context is in the form of validated customers’ identification and background information; as well as customer risk categorisation information. The following sections will elaborate the two types of supplementary benefits that belong to this category.

---

34 Nevertheless, it is important to appreciate that the presentation on relevant requirements will not be reiterating in detail the information that has already been extensively discussed in Chapter 6.
Chapter 7: Analysis of Supplementary Benefits

7.2.1. Leveraging Identification and Background Information

The first type of supplementary benefit in this category arises from the opportunity to leverage validated; accurate; and up-to-date customer identification and background information, made readily available for AML/CFT purposes. By having the opportunity to leverage various customer information possessing the above characteristics, organisations would be able to utilise them during the effort to enhance their business relationships with customers. This situation is especially useful in the event when customers’ business relationships could be brought to a level that would be more beneficial to the organisation, at a later period and when the need arises.

This supplementary benefit differs from the rest of the benefits that will be highlighted in this chapter, in that it is based solely on customer information. Therefore, this benefit should not be equated with the opportunity to leverage customer risk categorisation information for business purposes [see subsequent Section 7.2.2]. In this regard, this contrasting benefit can, in effect, be considered as utilising various customer information to conduct a multifaceted assessment process in order to derive customers’ level of riskiness. In other words, in order to generate customer risk categorisation, the aforementioned information will need to be used as an input to the assessments. Moreover, the benefit of leveraging customer identification and background information is not based on time-critical and event-based information either [see Section 7.6.1]. This is due to the appreciation that this type of information is mainly regarded as relatively constant in nature, in which denotes that they are less subjected to frequent changes and modifications.

The realisation of this supplementary benefit can be explained by the following example. By having the opportunity to access accurate; validated; and up-to-date information on their customers\(^{35}\), organisations will be able use this information as an input to gauge the possibility of business enhancement opportunities. Furthermore, they can also accurately communicate with the identified customers when a cross-selling or a marketing opportunity has been discovered. For example, a customer of a

---

\(^{35}\) This information can be in the form of customer’s full name; permanent and correspondence addresses; date of birth; nationality; occupation; monthly salary; name of employer; nature and location of business or self-employment; and contact phone number for home, office or mobile, etc.
certain age group having high monthly salary and a stable occupation, as well as residing in a location that is favourable to business, could be a possible candidate. In addition, with the ability to leverage accurate and up-to-date information (such as customers’ phone number, as well as their email or postal addresses), the organisation could effectively and conveniently communicate with these targeted customers, whenever needed. This information may be used as a channel to inform the potential candidate about any business offers, promotional campaigns, etc.

In relation to the associated regulatory requirements that are considered to have influenced the realisation of this supplementary benefit, similar requirements were also found to be influencing several compliance benefits. As depicted in Figure 7-1, this supplementary benefit can therefore be regarded as having built upon compliance benefits relating to: customer validation; information reliability; discrepancies in financial transactions; customers from countries under observation; matching of names under surveillance; as well as differential engagement strategy. Detailed discussions on these requirements, regarded as ensuring customer information is efficiently obtained and maintained, are available in Appendix X.

It is interesting to note, however, regarding the absence of specific interview statements that have explicitly associated the requirements to obtain and maintain extensive customer information for AML/CFT, with the realisation of supplementary benefit. One plausible explanation can be attributed to the situation where the need for detailed information has already been well embedded in the organisation’s normal business processes. Hence, this particular situation has resulted in the research participants not being able to explicitly distinguish the specific information required for regulatory purposes, from the ones required by business.

This rationalisation can be further supported by instances when the researcher was trying to detect specific information driven by AML/CFT requirements, that had been included in the list of information to be obtained from customers during the opening of an account. In this regard, all interviewees were seen as not being able to fully recall the rationale for such information to be solicited in the first place, as it was said to have been implemented, for quite some time, in the past. In addition, when Bank
A’s opening of account forms [D016] were subsequently reviewed by the researcher, it was not possible to clearly distinguish between the information that can be classified to be solicited for AML/CFT, or required by business.

It may further be acknowledged that some form of customer identification and background information should have already been gathered for business intentions. Therefore, it can safely be assumed that part of the information required by regulations should also be available, and further being harvested as part of a normal business practice. On the other hand, it is important to reiterate the importance of obtaining and maintaining validated; accurate; and up-to-date customer information, at the extent suggested by the requirements [see Appendix X]. Failing or lacking to do so will definitely expose the organisation to various adverse repercussions by the regulatory authority [see examples in Section 5.4.1(b)].

Therefore, it can be safely be concluded that regulatory requirements have indeed provided a *strong driving force* to obligate organisations to obtain and maintain extensive customer information for regulatory purposes. Hence, this situation has consequently presented the opportunity for organisations to conveniently leverage this information for business. Furthermore, an organisation’s recommended business practice to gather and maintain detailed customer information may not guarantee the intended dedication and commitment. This can be due to the understanding that failure to especially maintain the currency of customer information may only resulted in a missed business opportunity, without having to endure possible penalties by the regulatory authority.

Nevertheless, having recognised and rationalised the lack of specific statements from interviewees from banking institutions, it may be worth noting the insights provided by a Deputy Director from the regulatory authority. In this regard, the interviewee can be regarded as *acknowledging* the potential business benefits from validated, accurate, and up-to-date customer information gathered for AML/CFT. Although the interviewee was not able to recall the names of any of the institutions (and therefore has made further verification infeasible), it had nevertheless presented a useful
example how organisations could possibly leverage customers’ information to strategise their marketing efforts:

“I know when I spoke to at least 3 banks, these are local banks as well as foreign banks, they said having to ask their customer more information at the early stage of opening of accounts because of the requirements under AMLATFA, it helps them to understand their customers and they actually re-strategised their marketing based on that information that they gather. So these are benefits that was not planned, but as a bank, as a business, some of them used these data in order to target what types of products for example to market based on the segment of income, etc.” (016)

Furthermore, in a slightly different perspective, Bank A’s IT Department lead for the RSA2 system had also highlighted the value that an AML/CFT IT system could bring to the organisation. The value is achieved through possessing rich and up-to-date information, gathered due the need to comply with AML/CFT requirements. Thus the following statements can likewise be regarded as indirectly supporting this supplementary benefit:

“If we can actually keep our data up to date, it really helps not just for marketing purposes, but for other reports that always want the most recent data.” (018)

In summary, supplementary benefit arising from the opportunity to leverage validated; accurate; and up-to-date customer identification and background information can therefore be achieved through the implementation of AML/CFT efforts within the organisation. In this regard, the above discussions have sufficiently elaborated the realisation of this particular supplementary benefit, through the rationalisation provided, as well as the appreciation on the associated requirements and insights from the interviewees. Table 7-1 provides a structured summary to the above discussions, pertaining to this specific supplementary benefit:
### Table 7-1: Benefit of Leveraging Identification and Background Information

<table>
<thead>
<tr>
<th>Factor</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>What</td>
<td>• What is the description of the supplementary benefit?</td>
<td>• Opportunity to leverage validated; accurate; and up-to-date customer identification and background information gathered for AML/CFT purposes to alternatively be used to benefit business.</td>
</tr>
<tr>
<td>Why</td>
<td>• Why is the supplementary benefit feasible?</td>
<td>• The supplementary benefit is feasible through the opportunity to broaden the usage of information gathered for regulatory purposes to provide additional value to the organisation. This is achieved by means having the opportunity to increase organisational effectiveness in enhancing their business with customers, especially in the event when a particular customer’s business relationship could be brought to a level that would bring more revenue to the organisation.</td>
</tr>
<tr>
<td>Where</td>
<td>• Where is the supplementary benefit arising?</td>
<td>• The supplementary benefit is detectable within the various business IT systems in the organisation that are used to capture and manage business interactions with the customers, catering for numerous banking products and services.</td>
</tr>
<tr>
<td>When</td>
<td>• When will the supplementary benefit be realised?</td>
<td>• The supplementary benefit will be realised immediately from the various business IT systems capturing and maintaining customer identification and background information.</td>
</tr>
<tr>
<td>Who</td>
<td>• Who (or which party) will have access to the supplementary benefit?</td>
<td>• The organisation’s business departments will have access to this supplementary benefit.</td>
</tr>
<tr>
<td>How</td>
<td>• How will the supplementary benefit be made available? • How useful is the supplementary benefit in contrast to alternative benefits?</td>
<td>• The supplementary benefit will typically be made available electronically, within the organisation’s business IT systems. • The supplementary benefit is extremely useful as organisations are obligated to obtain and maintain validated, accurate and up-to-date customer information due to the potential regulatory penalties, and thus somewhat guarantees its reliability.</td>
</tr>
</tbody>
</table>

### 7.2.2. Leveraging Riskiness Information

The second type of supplementary benefit in this category arises from the opportunity to leverage customer risk categorisation information, made readily available for AML/CFT purposes. By having the opportunity to leverage information pertaining to customer riskiness, organisations would be able to utilise this knowledge as one of the considerations to assess customer’s feasibility for an enhanced business relationship. Specifically, the information could be used as one of the inputs to help ascertaining...
customer’s suitability for potential cross-selling, promotional campaign, differential pricing, etc., when the opportunity arises.

It needs to be noted that the risk categorisation developed for AML/CFT serves a special purpose in contrast to the typical risk classification or scoring that would normally be employed within the business context. While the former risk categorisation explicitly measures customer’s riskiness to ML/TF, the latter is largely pointing towards the risk of customer defaulting on a credit extended by the organisation. Hence, from the business viewpoint, this particular risk scoring is typically concentrating on establishing customer creditworthiness, deriving from past credit history, as well as, anticipating possible future inclinations to the customer’s credit behaviour.

Importantly, it needs to be appreciated as well that customer risk categorisation for AML/CFT does not necessarily need to be premised on an established customer lending relationship with the organisation. As can be later appreciated through one of the interview statements being highlighted in this section, customer risk scoring developed for the purpose of business is, in effect, considered an after event. In this regard, organisations can only be able to generate the necessary information based on historical information arising from an existing or past business relationship with the customer.

Therefore, the risk categorisation from the perspective of AML/CFT can be considered as a valuable input to the feasibility assessments of a customer. In this regard, it should be used in conjunction with the typical business risk categorisation (as well as in other available measurements) in order to provide a critical added dimension in determining the customers that would be appealing to business. Furthermore, this supplementary benefit would also be deriving from the understanding that the input from AML/CFT perspective will be able to assist in mitigating the risk of abetting ML/TF activities through the organisation’s daily business dealings and interactions with the customer.

Moving the discussion on the distinctiveness of this supplementary benefit, it should be regarded as being different from the rest of the benefits in this chapter. This
situation is arising from the appreciation that this benefit emerges solely from customer risk categorisation information developed for AML/CFT. Therefore, this benefit should not be considered similar to the one discussed in the preceding Section 7.2.1, i.e. pertaining to the opportunity to leverage customer identification and background information. Briefly reiterating the earlier explanation, the contrasting benefit has been considered as the prerequisite condition to establish risk categorisation information. Therefore, information on riskiness is regarded as being made possible, as well as being an outcome to the organisations’ ability to firstly obtain the required information from their customers. In addition, this benefit should also not be regarded as having similarity to the benefit arising from time-critical and event-based information as well. As will later be explained in greater detail in Section 7.6.1, this particular benefit has no relation with the opportunity to leverage customers’ financial transactions that have been regarded as not being associated with ML/TF (i.e. the false positive alerts).

The potential realisation of this supplementary benefit would be best illustrated using the example used in the earlier Section 7.2.1 regarding the detection of a targeted category of customers (i.e. from a particular age group; with high monthly income; stable occupation; and resides in a favourable location). In this situation, it would be further reassuring for the organisation to target a specific customer for business enhancement activities, arising from the knowledge that the customer is deemed to be having lower riskiness to ML/TF. Therefore, the customer might be considered as more favourable, as compared to other customers that might be having relatively higher riskiness to ML/TF, but coming from the same identified category of customers. By choosing this particular customer, the organisation would be deemed to be able to mitigate the risk of dealing with customers that have higher chances of being associated with ML/TF activities. Furthermore, it is important to appreciate that the risk categorisation would also need to be regularly updated arising from changes in the customer’s information. Hence, organisations will likewise have the opportunity to apply informed judgement in determining whether a particular customer would be still deemed as favourable arising from possible changes to the riskiness to ML/TF.
In relation to the associated regulatory requirements that are considered to have influenced the realisation of this supplementary benefit, similar requirements were also found to be influencing several compliance benefits in Chapter 6. As depicted in Figure 7-1, this supplementary benefit can therefore be regarded as having built upon compliance benefits pertaining to: customer risk profiling; and differential engagement strategy.

Moving on to appreciate the views, opinions and standpoints of the research participants, several interviewees had offered useful insights that point towards to the realisation of this supplementary benefit. In this regard, the Head of Operations Risk and Compliance from a local banking institution had suggested about the potential of using lower customer risk scoring as a basis to enhance the business relationship with customers:

“So from day one, you can apply this [scoring] to every customer actually, when you start scoring on the location... from which location is the guy, what kind of business he is doing... So you can assign a score. If you find all these are low scores, and it ties in with the business nicely, if they got a lot of money, then you can do something about it.” (022)

In addition, Bank A’s Head of AML/CFT and Compliance Strategy had also highlighted the opportunity to leverage the information on customers to benefit business in terms of marketing to those that have been classified as low-risk:

“If let’s say this customer’s transactions, maybe probably we classify under high net worth customer, and they are clean. The risk profiling shows that they are low, you know, in terms of risk. So I suppose business should leverage these customers to do their selling... marketing...” (034)

Interestingly, it was also discovered that the President and CEO of Bank A had also specifically mentioned (i.e. during a presentation in an international conference pertaining to ML/TF) about the opportunity to conduct cross-selling from a category of customers that have been classified according to the AML/CFT requirements. As noted in one of the presentation slides used for the above conference [D017], it was found out that Bank A has considered the ability to classify customers as high net
worth and lower risk customers to ML/TF as providing value to the organisation. This value is in the form of having the opportunity to improve customer service and increase profitability through the ability to leverage customers having lower risks and subsequently deploy possible cross-selling initiatives.

On another note, it is essential to compare the general difference between AML/CFT risk categorisation and the risk scoring from the perspective of business. As importantly highlighted by Bank A’s Head of CRM, customers that have yet to establish a lending relationship with the organisation could not be assigned with a risk score (i.e. from a business point of view), as they do not have the necessary historical information:

"You see the risk score is an after event, meaning when the customers come in and they apply for a housing loan, and all that... If they happened to have a housing loan or a loan with us earlier on, then the risk score comes into the picture. But if they don’t have, then there is no risk score. Because the risk score is basically for a lending relationship.” (024)

In contrast, customer risk categorisation for AML/CFT does not necessarily need to be premised on an established customer lending relationship [see suggested criteria in Section 6.4.1]. Therefore, this type of riskiness information can be regarded as largely predictive in nature, since it is not based on known historical customer information available within the organisation. Hence, this particular situation justifies the need for an added dimension to be incorporated within the customer feasibility assessments being adopted by business.

To summarise, supplementary benefit arising from the opportunity to leverage customer risk categorisation information can thus be achieved through the deployment of AML/CFT efforts within the organisation. Table 7-2 provides a structured summary to the above discussions, pertaining to this specific supplementary benefit:
Table 7-2: Benefit of Leveraging Riskiness Information

<table>
<thead>
<tr>
<th>Factor</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>What</td>
<td>• What is the description of the supplementary benefit?</td>
<td>• Opportunity to leverage customer risk categorisation information made available for AML/CFT purposes to alternatively be used to benefit business.</td>
</tr>
<tr>
<td>Why</td>
<td>• Why is the supplementary benefit feasible?</td>
<td>• The supplementary benefit is feasible through the opportunity to broaden the usage of information established for regulatory purposes to provide additional value to the organisation. This is achieved by means of having the opportunity to utilise knowledge on customer riskiness as one of the considerations to assess customer’s feasibility for an enhanced business relationship.</td>
</tr>
<tr>
<td>Where</td>
<td>• Where is the supplementary benefit arising?</td>
<td>• The supplementary benefit of leveraging customer risk categorisation is detectable in the organisation’s AML/CFT IT system.</td>
</tr>
<tr>
<td>When</td>
<td>• When will the supplementary benefit be realised?</td>
<td>• The supplementary benefit will be realised immediately from the AML/CFT IT system subsequent to the risk rating calculations.</td>
</tr>
<tr>
<td>Who</td>
<td>• Who (or which party) will have access to the supplementary benefit?</td>
<td>• The organisation’s Compliance department (and business departments, with permission) will have access to this supplementary benefit.</td>
</tr>
</tbody>
</table>
| How    | • How will the supplementary benefit be made available?  
• How useful is the supplementary benefit in contrast to alternative benefits? | • The supplementary benefit will typically be made available electronically, within the AML/CFT IT system.  
• The supplementary benefit is extremely useful as organisations are obligated to establish customer risk profiling information due to the potential regulatory penalties, and thus somewhat guarantees its availability and reliability.  
• In addition, by utilising this information, it will provide a critical added dimension in the effort to determine whether the customers would be appealing from the perspective of business. Furthermore, it will also be able to mitigate the risk of the organisation being considered abetting ML/TF activities. |

7.3. SELECTIVE CUSTOMER BENEFITS

The second category of supplementary benefits outlines the business gains and advantages arising from the opportunity to leverage related screening process established particularly for AML/CFT. This particular supplementary benefit is achieved when the screening mechanism is used as a justification to be selective on
the type of customers that the organisation wishes to accept and maintain. The following section will elaborate this particular supplementary benefit in detail.

### 7.3.1. Leveraging Opportunity to be Selective

As briefly mentioned earlier, this type of supplementary benefit arises from the opportunity to leverage customer screening process that was established to mitigate the risk of ML/TF activities. Therefore, by leveraging AML/CFT customer screening, organisations would be able to provide one of the justifications for rejecting unwanted customers, and hence having the opportunity to be selective on the type of customers that the organisation wishes to accept and maintain.

The customer screening process, in this regard, is in the form of deploying proper CDD against customers wishing to establish banking relationship, and utilising this avenue reject undesired new customers not meeting the requirements. The CDD process is to be applied during opening of new banking account or establishing new banking relationship with customers. In addition, a similar form of rejection, i.e. in this case a termination of business relationship, can also be applied to undesired existing customers. This situation arises when the existing customers had failed to meet the organisation’s CDD requirements, especially in the effort to ensure the reliability and applicability of updated customer information.

Therefore, against this backdrop, and from the context of supplementary benefits, the CDD process can be used as one of the formal justifications to decline or refuse customer applications to engage with the organisation. Hence, a selective customer screening process premising on criteria set by regulatory requirements can be exploited to attain business benefits, in selecting new and maintaining existing customers of the organisation. In addition, organisations would also have the opportunity to focus and concentrate their organisational efforts on further enhancing business relationships with valued residual customers that have been retained. This can be done once business relationships with any undesired customers have been ceased and terminated according to AML/CFT measures.
Moving the discussion to distinctiveness, this supplementary benefit should be regarded as dissimilar from the rest of the benefits being presented in this chapter. This situation can be attributed to the understanding that other compliance benefits do not explicitly provide an avenue for the organisation to terminate customer business relationship arising from issues pertaining to ML/TF. In addition, while most of the supplementary benefits in this chapter tend to focus on discovering customers for business enhancement activities, this particular benefit is primarily concentrating on the opportunity reduce the number of unwanted customers.

Furthermore, it is important to note that this supplementary benefit differs from the opportunity to leverage customer risk categorisation information established for AML/CFT purposes [see Section 7.2.2]. From the context of risk categorisation, the supplementary benefit can be considered as a filtering mechanism to identify organisational customers that are having lower risks to ML/TF. More importantly, the result of customers being categorised as high-risk do not imply that their relationships with the organisation are to be ceased sometime in the future. In contrast, AML/CFT customer screening process is instead being used to sieve unfavourable customers that are deemed unsuitable or detrimental to the organisation. Therefore, while it would not be sensible to use risk categorisation information to support the decision to terminate customer relationships, the screening process on the other hand, is able to effectively provide the rationalisation for organisations to achieve this objective.

As depicted in Figure 7-1, this supplementary benefit builds upon compliance benefits pertaining to: customer validation; information reliability; termination of business relationships; and matching of names under surveillance. In addition, it is also being influenced by the need to establish the prerequisite underlying information infrastructure. Detailed discussions of these requirements can be found in the relevant sections in Chapter 6.

Moving on to appreciate the views, opinions and standpoints of the research participants, several interviewees had offered useful insights that point towards the realisation of this supplementary benefit. In this regard, research participants had indeed related the benefit of having the opportunity to conduct business with
Chapter 7: Analysis of Supplementary Benefits

integrity through having the ability to weed out unwanted customers. For example, Bank A’s Head of AML/CFT and Compliance Strategy had provided confirmation on the organisation’s ability to exit customer relationships based on AML/CFT requirements, which will therefore assist in obtaining (and retaining) customers that are valuable to the organisation:

“It would assist us to get good customer, proper customer, meaning if we know that the customer is doing business that we consider as, probably be termed as illegal whatever, we can actually exit the customer faster.” (003)

In addition, Bank B’s Vice President for Consumer Bank Risk Monitoring was also of a similar opinion to the above statement. The interviewee had suggested that implementing AML/CFT measures would facilitate interactions with high quality customers:

“The other thing I think this is where you tell the customers, in a way, unofficially, we only entertain people who can do good business dealings with us. We don’t want people who deal in anything that are irregular.” (006)

In a similar vein, it has interestingly been noted that Bank B’s Head of Retail Banking had seemed to be appreciative on AML/CFT implementation. In this regard, the interview had acknowledged that arising from AML/CFT deployment, the organisation was able to conduct business with integrity, which is considered to be the foundation for banking business. The interviewee had made the following statement when asked about the AML/CFT implementation from the viewpoint of a business department:

“Anti-money laundering from business point of view, what do you see? Well couple of things, number one obviously we want to do business with integrity. You know integrity and reputation is a fundamental foundation of banking.” (039)

Furthermore, Bank B’s Project Manager from Transformation Office had explicitly highlighted the opportunity to weed out unwanted customers through AML/CFT implementation, and similarly echoed the earlier statement that had suggested that organisations will be able obtain (and retain) customers that are valuable to the
organisation. The following two statements from the same interviewee had emphasised these assertions:

“By complying with this Bank Negara’s [central bank’s] requirements, we are able to weed out those customers that don’t fall into the category that we want to deal with. Most people who are involved in these things won’t really be a valuable customer of the bank.” (042)

“It’s good that we are able to weed out these things so that more effort, focus and resources can be channelled towards the customers that we want to deal with in the first place. Chances are, this is the one that’s going to bring the most benefit to the bank.” (042)

Moreover, it may be worth noting that the similar sentiment can also be detected through the statements made by a Manager from the regulatory authority. The interviewee had explicitly highlighted the benefit of obtaining business from good customers and ability to decline the unwanted ones, through the implementation of AML/CFT IT systems in the organisations:

“Because you invest in the system, you have a robust detection rule. You also benefited from it, in terms of business purposes, so you will get business from good people. At the same time you are able to catch or turn away bad people.” (032)

In a nutshell, supplementary benefit arising from the opportunity to deploy selective customer relationships can therefore be achieved through the implementation of AML/CFT efforts within the organisation. In this regard, the above discussions have sufficiently showcased the realisation of this particular supplementary benefit, through the rationalisation provided, as well as the appreciation on the associated requirements and views from the research participants. Table 7-3 provides a structured summary to the above discussions, pertaining to this specific supplementary benefit:
Chapter 7: Analysis of Supplementary Benefits

Table 7-3: Benefit of Leveraging the Opportunity to be Selective

<table>
<thead>
<tr>
<th>Factor</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>What</td>
<td>• What is the description of the supplementary benefit?</td>
<td>• Opportunity to utilise AML/CFT screening process to effectively be selective on the type of customers that the organisation wishes to accept and maintain.</td>
</tr>
<tr>
<td>Why</td>
<td>• Why is the supplementary benefit feasible?</td>
<td>• The supplementary benefit is feasible since the deployment of selective customer relationship would allow organisations to concentrate their efforts in enhancing business relationships with valued residual customers. This can be done subsequent to the termination of business relationships with unfavourable new and existing customers.</td>
</tr>
<tr>
<td>Where</td>
<td>• Where is the supplementary benefit arising?</td>
<td>• The supplementary benefit is detectable with the branches and departments that verify the feasibility, as well as regularly deals with organisational customers. In addition, the benefit is also residing in the customer screening process adopted by the organisation.</td>
</tr>
<tr>
<td>When</td>
<td>• When will the supplementary benefit be realised?</td>
<td>• The supplementary benefit will be realised upon the utilisation of AML/CFT screening process within the selection and management of organisational customers.</td>
</tr>
<tr>
<td>Who</td>
<td>• Who (or which party) will have access to the supplementary benefit?</td>
<td>• The organisation, in general, as well as in specific, the departments or branches responsible to verify and regularly deals with the customers.</td>
</tr>
<tr>
<td>How</td>
<td>• How will the supplementary benefit be made available? • How useful is the supplementary benefit in contrast to alternative benefits?</td>
<td>• The supplementary benefit will be made available through the output from the screening process of organisational customers. • The supplementary benefit is useful and critical, as it can be used as one of the various justifications to reject, terminate and maintain business relationship with organisational customers that may be a threat to the organisational image and reputation, through their suspected activities related to ML/TF.</td>
</tr>
</tbody>
</table>

7.4. FRAUD MITIGATION BENEFITS

The third category of supplementary benefits outlines the gains and advantages arising from the opportunity to leverage functionalities for monitoring and detection of fraud activities that are commonly made available within the AML/CFT IT system. The following section will elaborate this particular supplementary benefit in detail.
7.4.1. Leveraging Fraud Functionalities

As mentioned above, this type of supplementary benefit arises from the opportunity to leverage the functionalities for fraud monitoring and detection. The supplementary benefit is achieved when the extra functionalities inside the AML/CFT IT system are used to reduce any financial losses arising from fraudulent activities occurring within the organisation. Since fraud functionalities are not part and parcel of the requirements to deploy AML/CFT measures within the organisation, the usage of these functionalities has brought benefit to the organisation. The benefit is in the form of protecting the organisation’s profits from possible monetary losses due to fraud.

It needs to be emphasised that utilising fraud monitoring and detection functionalities within the AML/CFT IT system should not be equated to the scope of research objective RO2a [see Section 3.3.2]. To briefly reiterate, RO2a aimed to explore an organisation’s deliberate actions in responding to regulatory requirements that directly benefit the business. This is done by deploying supplementary business related activities, such as incorporating optional changes or considerations in the deployment of regulatory IT implementations. For example, as suggested by the literature, this aim can be achieved by combining tactical business requirements with strategic performance opportunities; deploying dual purpose of compliance spending (Garcia, 2004); or implementing holistic compliance processes (Volonino et al., 2004).

Nevertheless, it needs to be critically noted that although fraud functionalities can be considered as optional, in the above context, they are in effect commonly seen as one of the primary components in a typical AML/CFT IT system solution provided by IT vendors [see Section 5.4.3]. Therefore, the utilisation of these extra functionalities should be more regarded as a logical action, rather than having the tendency to be considered as a deliberate and planned activity to directly benefit business. Hence, it should be regarded as a sound practical judgement for institutions to use the extra functionalities on fraud monitoring and detection that are already typically made available within an IT solution being deployed for regulatory purposes.
Chapter 7: Analysis of Supplementary Benefits

Furthermore, both fraud and AML/CFT functionalities can also be considered as a form of risk mitigation. In this regard, it can be considered that the main intention of deploying these functionalities is to reduce the risks of possible fraud, as well as ML/TF activities occurring within the organisation. Therefore, the opportunity to protect organisation’s profits from possible monetary losses due to fraud, in this context, can be seen as more of an indirect benefit. It is a resulting outcome from the deployment of fraud risk mitigation efforts, and hence, should not be regarded as deliberate action to directly benefit the organisation’s business.

In relation to the discussion on distinctiveness, this supplementary benefit should be regarded as dissimilar from the rest of the benefits being presented in this chapter. This situation is due to the understanding that this particular benefit arises from the utilisation of system functionalities that are not related to AML/CFT. In addition, it has no relation with the various opportunities to leverage ML/TF activities and directly benefit banking business (i.e. such as in Sections 7.2.1; 7.2.2; and 7.3.1).

Importantly, it can also be similarly highlighted that there is an absence of specific requirement in the guidelines and legislation on AML/CFT that could directly be associated with fraud monitoring and detection activities. Nevertheless, it can be regarded that in order for these activities to be effective, validated; accurate; and up-to-date customer identification and background information is definitely essential [see Section 7.2.1]. Therefore, this supplementary benefit can also be generally associated with the compliance benefits arising from the need to obtain and maintain extensive customer information.

This supplementary benefit can be further appreciated by illustrating the underlying concepts for both functionalities, AML/CFT and fraud. As it is generally known, money laundering can be fundamentally described as the process of transforming proceeds obtained from illegal activities and attempting to conceal their true origin by disguising them as if have been generated from legitimate sources (Le-Khac et al., 2009) [STG, section 3.1.1]. In contrast, fraud (i.e. in specific context to the banking

---

36 On the other hand, terrorism financing is any activity to financially supplement terrorist related activities, regardless of whether the original source of funding has been considered as legitimate or otherwise.
environment) can be generally explained as the deceiving act of stealing or pilfering legitimate funds to illegally benefit certain individuals or parties. Hence, in the case of fraud incidences, the original funds are legitimate (as opposed to the illicit money laundering proceeds) but have however been unlawfully acquired.

Moving on to appreciate the *views, opinions and standpoints of the research participants*, several interviewees had offered useful insights that point towards a rationalisation of this supplementary benefit. In specific relation as to why it is considered sensible to leverage fraud functionalities in the AML/CFT IT system, a CIO of a local banking institution had provided an excellent insight into this topic. The interviewee had suggested that it is logical to look at other options such as fraud, when implementing newer AML/CFT IT systems:

> “If you look at some of the newer compliance systems, they ride on the fact that when you do compliance tracking you actually pick up a lot of potentially useful information. And therefore you can logically look at option such as fraud reporting, internal fraud, you can look at besides anti-money laundering” (038)

Nevertheless, although the above statement have presented useful justification on organisation’s policy to leverage the extra functionalities on fraud, it is essential to appreciate as well the reason why these two functionalities were typically amalgamated in a single regulatory IT system in the first place. In this regard, within the effort to detect ML/TF activities, it is important to reiterate that the AML/CFT IT system mainly analyses granular customer information, which are at the level of banking transactions [see also Sections 5.3.2; 7.5.1; and 7.6.1]. It is further essential to appreciate that functionalities for fraud are in effect, analysing similar banking transactions, as well. Therefore, both functionalities correspondingly require continuous monitoring of customers’ transactional information in order to be significantly effective in their detection capabilities. As explicitly mentioned by Bank A’s Head of Integrated Risk Management, transactional information can be treated as a prerequisite condition to AML/CFT and fraud monitoring and detection:
“So to do fraud and also AML detection, you actually need to know about the transactions patterns. So meaning that you have to actually bring in all the transactions.” (037)

Furthermore, a Compliance Manager from one of the local banking institutions had also shared the same opinion regarding both functionalities that are fundamentally using similar type of information:

“Both basically need more or less the same information. They analyse customer’s data, they analyse customers transactions and flows.” (015)

Therefore, through the combination of these functionalities, fraud monitoring and detection capabilities can also be regarded as utilising the efficiencies of AML/CFT IT system, i.e. by accessing readily available transactional information that have been established for AML/CFT. In addition, as related by Bank A’s Head of Analytics, fraud functionalities are considered an income generator, arising from the ability to mitigate possible monetary losses:

“The fraud prevention part is supposed to be the income generating part, I mean anything you save or prevent the fraud is actually income to you. “ (001)

The above view is echoed by an interviewee in Bank B. The Vice President for Consumer Bank Risk Monitoring also highlighted that the AML/CFT IT system could be utilised to detect fraud occurrences:

“You can leverage, for example we say, it may not be money laundering, it can be fraud. So we actually use the system to also to cater for fraud detection.” (006)

Nevertheless, it may be important to note that although fraud and AML/CFT functionalities are both examining customer transactions, they are in effect, utilising a different set of assessments to uncover any possible exceptions through their different analysis and detection standpoints. This particular condition can be further illustrated through the transactional information regarding customers’ deposits and withdrawals activities. For example, rapid deposits into and withdrawals from a customer’s account may highlight elements of suspiciousness as they may suggest
that a particular account is being used as a transit for ML/TF activities. On the other hand, sudden surge in customer’s withdrawals beyond a tolerable range (i.e. obtained through monitoring of customers’ transactional information from fraud perspective) may point towards elements of fraud occurrences, such as illegal fund withdrawal arising from an identity theft.

In connection to the above, the IT Department lead for the RSA2 system in Bank A had confirmed about the usage of similar transactional data by both AML/CFT and fraud components, but nevertheless using different business rules and generating dissimilar types of alerts and sets of reports:

“When it comes to data, yes, same data but different business rules are applied. So different alerts or different reports are generated.” (004)

In addition to the above understanding, it is important to appreciate that the supplementary benefit arising from fraud monitoring and detection is not only limited to cases pertaining to the customers of the organisation. In effect, it is also inclusive of fraud committed by bank employees (i.e. staff fraud), as well. As mentioned by Bank A’s Head of AML/CFT and Compliance Strategy, the AML/CFT IT system in Bank A is designed to capture abnormal staff activities that could point towards staff fraud incidences:

“We are using it also to monitor our staff behaviour in the sense that if they regularly do a balance enquiry on a customer, let’s say more than the normal [number of] times in a day... let’s say this particular teller is checking on the customers balance, for example, 20 times in a day. So that is something abnormal.” (034)

In regard to Bank B, the monitoring of staff fraud is also available in the organisation, as confirmed by the Vice President for Consumer Bank Risk Monitoring:

“And actually, [the system] checks our accounts, not only on customers but also our staff accounts, and where are the trends of operations.” (006)

In summary, supplementary benefit arising from the opportunity to leverage the extra functionalities for fraud monitoring and detection can therefore be achieved through
the implementation of AML/CFT IT system within the organisation. In this regard, the above discussions have sufficiently elaborated the realisation of this particular supplementary benefit. Table 7-4 provides a structured summary to the above discussions, pertaining to this specific supplementary benefit:

Table 7-4: Benefit of Leveraging Fraud Functionalities

<table>
<thead>
<tr>
<th>Factor</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>What</td>
<td>• What is the description of the supplementary benefit?</td>
<td>• Opportunity to effectively mitigate the risk of financial losses due to fraud by leveraging the implementation of AML/CFT IT system.</td>
</tr>
<tr>
<td>Why</td>
<td>• Why is the supplementary benefit feasible?</td>
<td>• The supplementary benefit is feasible as it provides organisations with the opportunity to safeguard organisational profit against financial losses due to fraudulent activities by customers, as well as by staff. This is achieved by the opportunity to leverage the functionalities on fraud monitoring and detection that are typically available within the AML/CFT IT system.</td>
</tr>
<tr>
<td>Where</td>
<td>• Where is the supplementary benefit arising?</td>
<td>• The supplementary benefit is detectable within the establishment of AML/CFT IT systems.</td>
</tr>
<tr>
<td>When</td>
<td>• When will the supplementary benefit be realised?</td>
<td>• The supplementary benefit will be realised a day after batch processing, and upon the utilisation of the fraud functionalities within the AML/CFT IT system.</td>
</tr>
<tr>
<td>Who</td>
<td>• Who (or which party) will have the access to the supplementary benefit?</td>
<td>• The organisation’s fraud monitoring team will have the access to this supplementary benefit.</td>
</tr>
<tr>
<td>How</td>
<td>• How will the supplementary benefit be made available? • How useful is the supplementary benefit in contrast to alternative benefits?</td>
<td>• The supplementary benefit will be made available through the fraud monitoring and detection functionalities within the AML/CFT IT system. • The supplementary benefit is extremely useful as it enables effective monitoring and detection of fraudulent activities, made possible through the implementation of AML/CFT IT system.</td>
</tr>
</tbody>
</table>

7.5. INFORMATION REPOSITORY BENEFITS

The fourth category of supplementary benefits describes the gains and advantages arising from the opportunity to leverage an IT repository established for regulatory purposes. The following section will elaborate in this supplementary benefit in detail.
7.5.1. Leveraging Regulatory IT Repository

The realisation of this supplementary benefit can be attributed to the understanding that transactional information needed for AML/CFT purposes is typically sourced from multiple business IT systems. The information is usually being made readily and easily accessible from a central location for the purpose of analysis and detection of suspicious activities. Hence, the business benefit in this perspective is in the form of utilising this readily available repository of *transactional* information in order to aid business banking directly. Furthermore, by doing so, organisations will also be presented with an opportunity to enhance the efficiency of their IS operations. This is achieved when other IT systems’ turnaround time is improved due to the permission allowing them to obtain required information from a central repository that has already been established and made readily available.

This arrangement would be in contrast to obtaining the needed information directly from various fragmented source systems with different data formatting, and subsequently undergoing labourious cleansing processes to ensure consistency and uniformity. In addition, extended benefits will also materialise when the IT repository is enhanced to incorporate transactional information for more banking products. The more wide-ranging customer transactions obtained from multiple IT systems that are able to be collated in the IT repository, the more effective the AML/CFT detection capabilities would be. Accordingly, the associated benefit in leveraging the AML/CFT IT repository experienced by secondary repository users will also be consequently extended, arising from the proliferation of information that can be used for purposes beyond meeting regulatory requirements. However, it may be worth noting at this stage that the supplementary benefit from leveraging an IT repository established for AML/CFT purposes is *not* to be confined only to a specific intention, such as to enhance customer relationships. Rather, this benefit can also be associated with the demands on customers’ transactional information from various departments or banking systems within the organisation for various reasons and intentions.

Moving the discussion to *distinctiveness*, this supplementary benefit should be regarded as being different from the rest of the benefits being presented in this
Chapter 7: Analysis of Supplementary Benefits

This situation can be attributed to the understanding that this particular benefit arises specifically from the opportunity to leverage cleansed transactional information directly from the IT repository established for AML/CFT purposes. This situation will be in contrast to other identified supplementary benefits, which are mostly being regarded as alternatively utilising the information that have been generated or produced through organisation’s AML/CFT efforts.

This benefit of leveraging regulatory IT repository can be further appreciated by the following example. This specific illustration aims to further explain the opportunity to increase the efficiency of organisation IS operations, arising from leveraging cleansed customer transactional information. In this regard, transactional information sourced from two or more banking systems (e.g. for current accounts; loans systems; etc.) will most likely be having different formatting standards and naming conventions. Hence, ensuring data uniformity and consistency when the transactional data are to be gathered for various purposes will typically require an onerous and thorough cleansing process. Therefore, with cleansed transactional information already being made available within the central repository for AML/CFT, the turnaround time for other IT systems requiring similar transactional information could significantly be reduced when they are allowed to access it from this regulatory repository. Furthermore, as transactional information from more banking products being added to the existing repository, the availability of cleansed and centrally located transactional information will be increased, and consequently could be leveraged to further benefit business.

In relation to the associated regulatory requirements that are considered to have influenced the realisation of this supplementary benefit, similar requirements were also found to be influencing one of the compliance benefits in Chapter 6. As depicted in Figure 7-1, this supplementary benefit is regarded as having built upon the appreciation on compliance benefits pertaining to the recommendations to establish organisation’s MIS for AML/CFT purposes. Detailed discussions on these recommendations are available in Chapter 6.

Moving on to appreciate the views, opinions and standpoints of the research participants, several interviewees had indeed offered useful insights that point
towards to the realisation of this supplementary benefit. However, it is essential to appreciate that this supplementary benefit is primarily realised only in Bank A. The reason as to why this particular situation has occurred can be appreciated by the various interview statements and rationalisation that will be presented in the following discussions.

In specific relation to Bank A, it has been discovered that the benefit of leveraging AML/CFT IT repository has indeed been achieved. In this organisation, the central repository of transactional information created for its RSA1 system had been leveraged by the Customer Relationship Management (CRM) department of the bank. Bank A’s Head of AML/CFT and Compliance Strategy had provided confirmation regarding the linkage between RSA1 and the system in CRM department. In this regard, transactional information from RSA1 has been used as an input to measure the possibility of enhancing business relationships with customers:

“Yes, they [i.e. the CRM department] are actually using our RSA1 data to do their data mining and cross-selling. So that is another benefit for the bank.” (034)

It is essential to note that the RSA1’s IT repository has, in effect, been considered as one of the main and critical informational feeds for the CRM department’s data mart [D018; D019]. In this regard, the transactional information is further being used by a system created to discover marketing opportunities, known as the CRM1 system. Since RSA1’s inception in 2006, the CRM1 system has been leveraging transactional information from RSA1’s central repository as one of its two key informational inputs (i.e. aside from the information obtained from the bank’s Group Data Warehouse).

The following two interview statements have underscored the importance of accessing customers’ transactional information for CRM department. As suggested by Bank A’s Head of CRM, appreciating customers’ transaction patterns is critical to enable deeper understanding on organisational customers:

“So when we want to understand our customer better, we need to know the pattern of customer transactions, or customers’ behaviour.” (024)
In addition to the above view, another interviewee had explicitly drawn attention to the need to understand customers’ activities in order to prompt appropriate marketing campaigns:

“We need to analyse on the activity of the customers so that we can trigger marketing campaigns.” (030)

Furthermore, the Head of National Leads highlighted that, by gaining access to transactional information from the RSA1 system, the information has been regarded as “a single source of truth” (030). This is arising from the appreciation that the cleansing process has indeed been implemented, in order to address issues pertaining to missing and incomplete data, as well as ensuring a consistent and coherent formatting. From the CRM department perspective, the RSA1 system has performed the gate keeper function in ensuring that the quality of data is at the highest level:

“Then on the data quality itself, because whatever coming from RSA1, of course they are not going to put in rubbish. So RSA1 has already done the gate keeping, the quality checking before it goes to CRM. So on our side, we can do away with that quality checking knowing what RSA1 has already put in. So RSA1 have provided us with the single source of truth.” (030)

It is critical to appreciate at this point on the underlying reasons as to why the CRM department had to leverage RSA1’s central repository for its transactional information needs in the first place. This situation lies within the unique nature of Bank A’s IT infrastructure. Historically, when RSA1 was to be established, transactional information required by this AML/CFT IT system was not readily available in a central location. Even Bank A’s GDW was not storing information at transactional level, as it was initially built to suit the purpose of management or regulatory reporting. Therefore, as suggested by Bank A’s Head of CRM, the data warehouse is said to be storing information in an “aggregated and summarised manner” (024).

The above situation regarding Bank A’s GDW is further confirmed during a review of a banking document that the researcher was able to gain access to [i.e. D018, p. 24]. In a diagram on the core logical architecture of the CRM1 solution, the diagram had indicated that information in Bank A’s GDW is indeed stored in an aggregated level, i.e.
containing information such as the demographic profile of customers; customer segmentation; customer profitability reports; and account information, etc. Meanwhile, in the same diagram, data extracted from RSA1’s repository had clearly been shown as providing the CRM department the source for customers’ transactions at a granular level from the associated banking products and channels.37

Continuing the discussion on the unique nature of Bank A’s IT infrastructure, arising from the unavailability of transactional information in a central repository, it was further revealed that a request was indeed submitted to the Data Warehouse team in Bank A. The request was for the Data Warehouse team to specifically create an organisational central repository of transactional information which contains normalised and consistent data. However, since the request came solely from RSA1 team to cater for RSA1 establishment (i.e. in absence of similar requests from other business functions or systems owners), the business feasibility to establish a centralised organisational repository could not be fully justified. As highlighted by Bank A’s Head of Integrated Risk Management, as a result, the RSA1 IT team was handed with the task to establish a this repository, but only specifically to cater for the needs of RSA1 system:

“Actually we approached them [i.e. the Data Warehouse team] first. We said, can we have a transactions data mart? But the Data Warehouse [team] mentioned that there are no [similar] requirements, so nobody asked for it. It’s only you, it’s only one group of users. Please handle it yourself.” (037)

Therefore, the establishment of a central repository for transactional information in Bank A has indeed been created through the RSA1 system deployment. As a consequence, subsequent request by the CRM department to access similar information was logically directed to this IT repository, and has resulted in the realisation of this supplementary benefit.

In addition, as related by Bank A’s Head of Integrated Risk Management, the transactional information within RSA1’s central repository is being stored in a

37 The customer transactions, in this regard, are for example pertaining to; withdrawals; deposits; fund transfers; bill payments; pre-paid purchases; cheque transactions; balance enquiries; teller transactions; etc.
“normalised” and “consistent definition” (037). Therefore, the CRM department was also able to obtain further benefit in the form of being cost effective, as well as having a speedier turnaround time. This situation can be contrasted with sourcing the needed information directly from the core banking system and various other fragmented systems in Bank A. The IT Department lead for the RSA2 system had, in two instances, mentioned about the challenges of cleansing the data that were attained from various organisational source systems, as well as the benefit experienced by the CRM department due to the quicker and easy access of required information made available through RSA1’s repository:

“...there a lot of different source systems in the bank, and to clean up is a massive exercise.” (018)

“Because you see, if they [i.e. the CRM department] were to go back to the core banking system, it would take longer. So current infrastructure [arrangement] is they are taking data from us [i.e. the RSA1’s repository] on daily basis.” (018)

Similar sentiment was also being echoed by an interviewee from the CRM department. The Head of CRM, in this regard, had distinctively highlighted the opportunity to avoid the need to go through the cleansing process again, in order to obtain the need information for CRM department’s purposes:

“It is a necessary thing to do because the source for current and savings, goes through that particular [cleansing] process. So it’s not effective for us to go through the current account and the savings systems [again]. Because if we go to current account and savings systems, then it’s a two ETL - Extract, Transform and Load – processes.” (024)

It is critical to note at this point that the information from RSA1 central repository which the CRM1 system was allowed to access is essentially the raw and unprocessed (albeit cleansed) transactional data which have yet to be analysed or screened for AML/CFT purposes. Therefore, any issues regarding confidentiality and sensitivity of AML/CFT related information being accessed by a non-designated department should not arise. In this respect, Bank A’s Head of Integrated Risk Management had provided
the assurance that the CRM1 system is merely assessing raw (but cleansed) transactional data from the RSA1 system:

“They [i.e. the CRM department] are only using the same input. That means it is actually the whole bank’s transactional data.” (037)

Therefore, in a nutshell, by accessing the information made readily available in RSA1’s central repository, the CRM1 system does not necessarily have to undergo a similar repetitive process in performing data cleansing all over again.

On a separate issue, but nevertheless, considered as an incremental discussion, it was also revealed by the IT Department lead for the RSA2 system that analysis conducted in RSA1 was rather limited. In this regard, the system is said to be “quite rigid” and “not flexible” (004), as well as only confining to “current, savings and all the e-channels” (018). Furthermore, Bank A’s Head of Group Compliance has also regarded the system to be “not that robust” (008) in the effort to cater for new requirements and new banking products. In addition, according to the Head of Analytics, RSA1 also suffers from “audit shortcomings” (001) arising from the outcome of a supervisory examination conducted by the central bank. Therefore, considering the above constraints affecting the RSA1 system, the management of Bank A had given the endorsement to replace RSA1 with a new AML/CFT system named RSA2.

It was revealed to the researcher that transactional information from Bank A’s six banking systems catering for various products will be added to the existing transactional information repository for current and savings accounts to cater for the new AML/CFT system needs and capabilities. These banking systems are for loans; credit cards; fixed deposits; auto finance; insurance; and stock broking. Therefore, as a result, the benefit experienced by the CRM department will be expanded due to an increase in the amount of cleansed and centrally located transactional information that would be made available to the CRM1 system. Accordingly, the analysis

\[\text{please note that most interviewees in Bank A would generally indicate that the RSA1 system as having information only for current and savings accounts. The e-channels transactional data mentioned by this interviewee is only referring to the means how transactions were conducted, and all information is said to eventually be recorded as transactions catering for current and savings accounts. Hence, for the purpose of clarity, and in line with the statements made by most interviewees, the discussion relating to RSA1 will only be mentioning these two accounts only.}\]
conducted by the CRM1 system to discover the possibility of enhancing business relationships with selected customers will be enhanced as well, since it will be premised upon customers’ transactional information from a wider number of banking products.

The information obtained from the follow-up phone interviews, during the supplementary phase, helped to provide an update of case A’s situation. It was revealed that although the RSA2 system has already been deployed, the CRM department is currently accessing the needed information directly from the core banking system, as an interim solution. The decision was made due to the different data formatting used by the RSA2 system:

“What they [i.e. the CRM department] have done is, instead of taking from RSA2 system, right now they are going direct to the host .... Because if they were to map to RSA2’s file format, it’s a massive work for them. So they are taking a quick win solution [at this moment].” (048)

However, since only limited information pertaining to “current, savings, and fixed deposits” (051) is being accessed from the core banking system, the CRM department is still interested to access transactional from the RSA2 system’s repository, as soon as possible:

“Yes they are [interested] because the RSA2 system has more products that they want to leverage .....” (048)

In addition, the following two statements from the Head of CRM Technology have provided excellent insights on the department’s interest and future plans:

“At the moment, the temporary solution is, the CRM1 system will be sourcing the data from host. So moving forward, the CRM1 system will be merging with the future regional data warehouse. In this data warehouse’s architecture, one of the sources [for transactional data] is from the RSA2 system.” (051)

“Even if the regional data warehouse does not materialise, we will still do the enhancement to access from RSA2. Because currently not all transactions are
obtained from host .... [we] will access more products from RSA2, such as loans, remittance and insurance.” (051)

Therefore, the above interview statements have provided assurance on the legitimacy of the supplementary benefit that has been identified in this section. This is albeit fully acknowledging the CRM department’s temporary interruption in accessing customer transactional information from the AML/CFT IT repository.

Moving the discussion to reflect on the situation affecting Bank B, it seemed that the supplementary benefit from leveraging regulatory IT repository has not being experienced by this organisation. This situation can be attributed to understanding that customer transactional information in Bank B is already available in the organisation’s Enterprise Data Warehouse (EDW). Even though a separate IT repository was created for its RSB1 system (which contains transactional information gathered from EDW and several source systems39), Bank B’s business departments were not tapping the repository built for AML/CFT to directly benefit banking business. This is due to the appreciation that the organisation’s transactional information, needed by the some departments for the purpose of business analytics, is said to be sufficiently available in Bank B’s EDW.

It may be worth reiterating at this juncture that Bank B’s has indeed established a separate IT repository for its RSB1 system. Therefore, this situation may indicate that customer transactional information required for AML/CFT purposes may not have been completely available in the EDW. Hence, the organisation’s contentment on EDW’s information sufficiency in serving business demands, may somewhat have resulted in a missed opportunity. In this regard, Bank B might be seen lacking to possibly leverage cleansed, as well as richer transactional information that might be available in RSB1’s repository (i.e. in relation to the information beyond the ones available centrally in the EDW).

Nevertheless, it is acknowledged that this type of supplementary benefit would most likely to be experienced by organisations that have yet to establish a comprehensive

39 Other source systems in this regard are; conventional banking; Islamic banking; auto finance; trade finance; credit card; and trading room systems.
central repository of transactional information during their AML/CFT implementations (like Bank A). Organisations possessing a similar historical nature affecting Bank A would therefore likely to be more inclined in leveraging any IT repository containing the needed information that has already and readily been established in their organisation.

It can also be further stated that Bank B was not experiencing an opportunity to enhance its IS efficiency through leveraging a central IT repository for AML/CFT. In this regard, the opportunity to leverage this repository can be considered as one of the preconditions for Bank B to further experience the benefit of reducing its IS operations’ turnaround time. Nevertheless, even though some form of IS operational efficiencies may have indeed been achieved through leveraging the central EDW, this form of efficiency has no relationship with attaining similar benefit from a regulatory driven IT system implementation.

The above situation has also prevented Bank B from appreciating further benefit whenever the capacity for the regulatory IT repository is expanded (like in Bank A). In this regard, the circumstance has resulted in the inability or missed opportunity for Bank B to encounter further supplementary benefit through accessing a more extensive transactional information. This is especially true whenever the repository is extended to incorporate transactional information for more banking products.

In summary, supplementary benefit arising from the opportunity to leverage regulatory IT repository to directly benefit banking business can therefore be achieved through the implementation of AML/CFT efforts within the organisation. Nevertheless, it is worth noting that this type of supplementary benefit is only related to Bank A, arising from its opportunity to leverage the AML/CFT IT repository, as well as its decision to enhance the transactional information by incorporating more banking products. Therefore, the above discussions have sufficiently elaborated the realisation of this particular supplementary benefit, through the rationalisation provided, as well as the appreciation on the associated requirements and insights from the interviewees. Table 7.5 provides a structured summary to the above
discussions, pertaining to this specific supplementary benefit by appreciating the situation specifically for Bank A:

Table 7-5: Benefit of Leveraging Regulatory IT Repository

<table>
<thead>
<tr>
<th>Factor</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>What</td>
<td>• What is the description of the supplementary benefit?</td>
<td>• Opportunity to leverage AML/CFT central repository of transactional information to directly benefit banking business; improve business IT systems turnaround time; and obtain information for more banking products due to system enhancement.</td>
</tr>
<tr>
<td>Why</td>
<td>• Why is the supplementary benefit feasible?</td>
<td>• The supplementary benefit is feasible through the opportunity to broaden the usage of regulatory IT repository to assist in possibly enhancing banking relationships. In addition, it also increases the efficiency of business IT systems in acquiring cleansed transactional information, as well as the ability to possibly obtain richer customers’ transactional information from additional types of banking products.</td>
</tr>
<tr>
<td>Where</td>
<td>• Where is the supplementary benefit arising?</td>
<td>• The supplementary benefit is detectable within the AML/CFT IT system’s central repository containing transactional data that has been cleansed and consistently formatted.</td>
</tr>
<tr>
<td>When</td>
<td>• When will the supplementary benefit be realised?</td>
<td>• The supplementary benefit will be realised a day after transactional information in the IT repository is made available after batch processing, and instantaneously accessed by the CRM1 system.</td>
</tr>
<tr>
<td>Who</td>
<td>• Who (or which party) will have access to the supplementary benefit?</td>
<td>• Bank A’s CRM department, i.e. owner of the CRM1 system, will have access to the supplementary benefit.</td>
</tr>
<tr>
<td>How</td>
<td>• How will the supplementary benefit be made available? • How useful is the supplementary benefit in contrast to alternative benefits?</td>
<td>• The supplementary benefit will be made available automatically through the regulatory IT repository, without manual intervention. • The supplementary benefit is extremely useful and critical, as the central repository containing cleansed customers’ transactional information is only available within Bank A’s AML/CFT IT system.</td>
</tr>
</tbody>
</table>

7.6. EVENT-BASED INFORMATION BENEFITS

The fifth and final category of supplementary benefits outlines the gains and advantages arising from the opportunity to leverage selected event-based customer transactional alerts generated by the AML/CFT IT system, and to directly benefit
banking business. The following section will elaborate in this supplementary benefit in detail.

7.6.1. Leveraging Time-critical Event-based Information

This supplementary benefit arises from the opportunity to leverage selected alerts generated by the AML/CFT IT system, which are specifically based on events detected through customers’ financial transactions. Therefore, this benefit is realised arising from the organisation’s ability to exploit selected daily customers’ financial activities that change frequently and rapidly, owing to them being actively observed specifically for ML/TF purposes. As depicted in Figure 7-1, this supplementary benefit can be regarded as building directly upon compliance benefits pertaining to: detecting discrepancies of customer’s financial transactions; violations in transactional threshold limits; and establishing organisation’s MIS for AML/CFT purposes, as well as indirectly influenced by the other remaining benefits.

Briefly reiterating the earlier discussion in Section 5.4.4(c), any discrepancies in customers’ financial transactions detected by the AML/CFT IT system will trigger event-based alerts. Upon deploying the needed assessment activity, i.e. the enhance CDD process, some alerts will eventually be considered as not being associated with ML/TF activities (i.e. regarded false positives). Therefore, these false alerts can also be considered as genuine financial events that may be time-critical in nature. Importantly, they can likewise be considered as abnormal financial transactions made by customers that have acted beyond their regular (and predictable) financial activities and behaviours.

Consequently, the discovery of these genuine financial events can also be regarded as possibly indicating specific instances of customer’s needs or demands. Therefore, they can indeed be utilised as an indicator for organisations to possibly pursue any business enhancement activities with these identified customers. In this regard, these

---

40 Event-based information can be explained as arising from a specific or a set of transactional activities made by a customer. In addition, due to their potentially brief and fleeting characteristics, in which business opportunity would be valuable for organisations to pursue further, the feasibility lifespan of the information can also be deemed as limited, and therefore be considered as time-critical in nature.
false alerts may be used as a signal to embark on such measures, as well as to be assessed further using other possible information to measure the feasibility of actions that should be taken in order to benefit banking business.

Furthermore, by pursuing to engage with these identified customers, organisations will also be able to significantly mitigate the risk of inadvertently dealing with customers that may later turned out to be associated with ML/TF activities. As these customers have been specifically identified through false positive AML/CFT alerts, organisations may be regarded as having another layer of assurance. This is arising from the understanding that they can be regarded as valuable customers that have been verified as not being associated with ML/TF activities. Indeed, the ability to mitigate any business dealings with customers that are associated with ML/TF activities is extremely critical to the business of the organisation. This is in view of the potential penalties that may be imposed by the regulatory authority, as well as the risk of adverse implications on organisation’s reputation [see Sections 5.4.1(b); and 6.6, respectively].

In relation to the discussion on distinctiveness, this supplementary benefit should be regarded as dissimilar to the rest of the benefits in this chapter. This situation can be attributed to its peculiarity in alerting possible business enhancement activities, which are contingent upon customers’ financial activities that are no longer being regarded as suspicious. Importantly, these event-based customer activities may also essentially be feasible only within a limited time frame. For that reason, this supplementary benefit arises from the organisation’s efforts to observe customers’ financial activities that change frequently and rapidly. Therefore, it is different to the benefit of leveraging information that is less susceptible to frequent changes [i.e. Section 7.2.1].

Furthermore, the benefit arising from the organisation’s opportunity to leverage customer risk categorisation information [see Section 7.2.2] does not generate the same level of advantage mentioned earlier in this section. This situation can be viewed from the perspective that AML/CFT risk categorisation will only allow the identification of customers that have less likelihood of being associated with ML/TF activities. Hence, the risk categorisation information provides less assurance that a
customer has any tendency to become unfavourable, as compared to the opportunity to explicitly exploit false positive alerts for similar purposes. Furthermore, false alerts provide the opportunity for the organisation to identify specific financial transactional event that has no relation to ML/TF activities, which could not be determined through leveraging the information on customer risk categorisation according to AML/CFT. Importantly, the ability to attain this supplementary benefit is uniquely associated only with AML/CFT false positive alerts. Therefore, it is critical to note that similar benefit would not be equally available in other types of exception reporting or flagging mechanisms employed by the organisation, for the purpose of regulation or otherwise.

This benefit of leveraging selected event-based customer transactional alerts can be further appreciated by the following example. Utilising the scenario provided in Section 7.2.2, assuming that a category of banking customers considered to be useful for the organisation’s business, and having lower risk to ML/TF, has been identified (e.g. from a particular age group; with high monthly income; stable occupation; resides in a favourable location; and having lower risk to AML/CFT). However, is critical to note that although customers from this category have been considered as safe and being sought after, no guarantee can be implied that they will never be involved in activities related to ML/TF in the future.

Nevertheless, during continuous monitoring, the financial transactions for one of the customers from the above category have been triggered by the AML/CFT system. In this regard, the incident was due to the discovery that this particular customer’s savings account has been deposited with a cheque worth RM200,000. The alert was due to the inconsistency with the financial profile of the customer (i.e. a bank officer with RM5,000 monthly salary). It was later found through an enhanced CDD process that the source of fund has been regarded as legitimate, and subsequently the alert has been classified as untrue (i.e. false positive). Therefore, specifically from the business perspective, the customer can now be considered as an excellent candidate for any possible business enhancement initiatives. This situation is especially arising from the organisation’s awareness of the availability of additional disposable fund.
Moving on to appreciate the views, opinions and standpoints of the research participants, several interviewees had indeed offered useful insights that provide the justifications and rationalisations for this supplementary benefit. However, it is essential to note at this juncture that this particular benefit has yet to be explicitly experienced especially by the two detailed case study organisations, Bank A and B. Nevertheless, through the appreciation on the information being revealed to, and discovered by the researcher, Bank A has been regarded as having much higher inclination to experience this supplementary benefit. In this regard, the tendency for Bank A to obtain this benefit primarily hinges on its propensity to leverage AML/CFT regulatory information as part of its structured and established organisational business practices. The situation affecting Bank A can be contrasted with the circumstances influencing Bank B, where the corresponding conditions and sentiments were deemed as absent or lacking, and hence was seen to be much less receptive and accommodative in achieving a similar objective.

The rest of the discussions pertaining to the insights obtained from the research participants will be adhering the following approach (which can be seen as being slightly different from the ones adopted by all the preceding discussions within this chapter). In this regard, it will initially present the various views and standpoints that had rationalise the potentiality of this supplementary benefit. Only then the discussion will focus on the contrasting situations and circumstances that had affected the two detailed case study organisations.

a) Feasibility in leveraging AML/CFT false alerts

There were various useful insights provided by the research participants that points towards the feasibility of this supplementary benefit. One of the best examples is arising from the statements made by the Head of Operations Risk and Compliance from a local banking institution. In this regard, the interviewee had indeed regarded as having introduced the notion of supplementary benefit arising from AML/CFT alerts that were considered untrue. This particular interviewee had interestingly suggested about customers’ transactions that were found to correspond with their profiles (i.e.
arising from the AML/CFT alerts) may in effect, present an excellent opportunity to be used to benefit business directly:

“...basically you’re looking at the KYC concept, know your customer. So KYC is actually looking at profiles, what’s the deposits, what kind of job he’s doing, what business, etcetera... So from there you can actually do the other way. Instead of looking at huge amount coming which doesn’t tie in with his pattern of transactions. But if it does tie and it’s a huge one [i.e. a significant amount], you may want to see how you may want to sell other things to the customer.” (022)

It may also be significant at this stage to appreciate the importance and criticality of event-based marketing from the perspective of business, as suggested by the above interviewee. In this regard, the Head of CRM from Bank A had provided another very useful insight into how this type of marketing approach was being deployed within the organisation. As noted by the two interview quotes below, this particular interviewee had explicitly mentioned about the value of understanding customer’s financial behaviours in order to facilitate the identification of discrepancies in transactions. The detection of these irregular transactional patterns would therefore be beneficial for the business in the form of triggering event-based marketing initiatives.41 This is arising from the understanding that it may be possible that the customer is in a “decision making mode”, contemplating to pursue further financial investments or engaging different types of banking relationships with the organisation:

“...what we did was we are able to track customers’ behaviour, in terms like their deposits. So we see that this customer has consistently putting in money, at every month, five thousands [Ringgit]. But suddenly, one particular month, and it’s not a bonus period or festival period, suddenly he put in fifty thousand [Ringgit]. So this is what we called the event-based marketing concept.” (024)

“So we will use all information that we have in relation to the financial information, whether their transactions, their card spent, their new purchases,

---

41 The term event-based marketing was discovered in document D018. In addition, the document had claimed that Bank A to be among the few pioneer institutions that have successfully deployed event-based marketing initiatives within the region, and the first Malaysian bank to implement such approach.
and all that. And when all this information are being put together, then we are able to trigger a moment where the customer is in a decision making mode. When that moment is being triggered then it is for us to immediately try to reach this customer and have a conversation, and try to understand their immediate needs and how we can help them. So that is event-based.” (024)

From the above statements, it may be fascinating to note about the similarity of approaches in detecting event-based marketing opportunities, with AML/CFT alerts to trigger potential ML/TF activities. In this regard, both perspectives are seen to be particularly interested in detecting, and subsequently reviewing abnormal financial transactions made by customers that have acted beyond their regular (and predictable) financial activities and behaviours.

Furthermore, the value of understanding and appreciating customers’ specific needs and demands, which may be relevant only in a specific time duration, was also pointed out by Bank A’s Head of National Leads. This particular interviewee had introduced the term “hot leads”, where the opportunity to engage with customers to address their pressing needs should be acted promptly, or else risking the chances of losing the potential business to the competitors:

“Because all these actions we called them as event-based, they are hot leads. Meaning to say, these customers are really in the need for something, so it’s better for us to call him fast, or else this customer would most probably end up with other banks. So the soonest we have it delivered to the branches, the better it will be.” (030)

Importantly, through a review of one of Bank A’s internal documents [i.e. D018] that the researcher had managed to gain access to, benefits arising from event-based oriented marketing efforts have indeed been noted. In this document obtained from the CRM department, it was said that this type of marketing approach enables various benefits, such as; “lower prospecting cost”; “better understanding of customer with smarter decision making”; “increase take-up rate”; and “fast and timely marketing campaign execution and improve campaign cost efficiency”. In addition, specifically regarding the opportunity to the reduce associated costs, it has been further
confirmed through a statement by an interviewee in Bank A. In this regard, the Head of CRM had explicitly highlighted the cost savings that can be achieved arising from a more focused and targeted marketing efforts:

“Knowing who the customer to target, is already a cost savings. Because they [e.g. the branches or marketing department] don’t have to go and search these customers.” (024)

Consequently, appreciating the above marketing approach being adopted by Bank A’s CRM department, and further compared with the uniqueness of AML/CFT false alerts, it is therefore sensible for organisations to consider the implementation feasibility of this particular supplementary benefit. Importantly, with the automation of AML/CFT efforts, speedy and timely analysis and generation of exception reporting, as well as prompt detection of suspicious activities can indeed be facilitated. Similarly, timely discovery of genuine customers’ transactions through false alerts can also be achieved, which will make the idea of leveraging false AML/CFT alerts more appealing and feasible to the organisation.

It was also interestingly discovered that generally, a predominant number of alerts generated by the AML/CFT IT system were indeed eventually regarded as untrue. For example, as related by Bank B’s Vice President for Consumer Bank Risk Monitoring, “about 10 percent” (006) of the total alerts generated by the RSB1 system is typically classified as suspicious, while the remainder 90 percent are therefore deemed as genuine transactions. Similarly, as highlighted by the Head of Compliance and Corporate Secretary from a foreign banking institution, about “80 percent” of the AML/CFT alerts in this organisation are also considered as false positives. This situation can be best explained by the insights provided by the Head of Group Compliance from a local banking institution. In this regard, the interview had suggested that it is completely acceptable for the AML/CFT IT system to produce huge number of false positive alerts as they are highly dependent on the parameters and scenarios that have been configured with:

“In any AML solutions also you will get a lot of false positives. Because the system is just a system, it doesn’t have a human brain behind it. So depending
on the parameter set and the scenario set, the more you put in, the more reports you would generate.” (020)

Nevertheless, it is important to appreciate at this juncture that the high number of false positives generated by the AML/CFT IT system should not be purely regarded as a sign of the system’s ineffectiveness. Rather, they should alternatively be viewed from the context that those detected transactions are truly arising from legitimate transactions and have been efficiently spotted by the system due to their rarity.

Therefore, having appreciated the feasibility of leveraging AML/CFT false alerts to benefit banking business, the following discussions will continue to explain this perspective from the context of Bank A and B. These discussions will provide the relevant justifications and rationalisations as to why one bank is seen to be more inclined to experience this benefit as compared to the other.

b) Bank A

In the case of Bank A, the organisation has been viewed as projecting a more positive outlook with regards to the possibility of realising this supplementary benefit. As mentioned earlier, this is arising from the organisation’s tendency to leverage AML/CFT regulatory information as part of its structured and established business practices. Overall, Bank A had been seen to be more attracted to the notion of leveraging information established for regulatory purposes and further to aid and benefit business. This peculiar situation exhibited by Bank A is over and above to the IT infrastructure linkage already been established between its AML/CFT IT repository and the CRM1 system owned by a business department [see Section 7.5.1]. The discussions that follow will justify this assertion in detail, by outlining the various underlying reasons and motivations that are affecting and influencing Bank A to plausibly pursue this path.

Firstly, and importantly, interviewees from Bank A’s Compliance department were seen to be far more receptive to the notion of leveraging regulatory information to aid and benefit business. For instance, it is fascinating to note that the organisation’s Head of Analytics had unprecedentedly mentioned about the potential marketing
benefits arising from an accomplished effort of collecting and storing customers’ information into a single IT repository that was established due to regulatory purposes:

“I think the best part is when we put all the data together. We can actually use the same data for marketing purposes also. I think because compliance on its own doesn’t generate any income to the bank. You’re just spending for nothing. So since the effort is already put in there, the data are already in one place in single data storage.” (001)

Additionally, the same interviewee had further suggested about the notion of maximising the investment of the new AML/CFT IT system, when explaining about the implementation of RSA2 system in Bank A:

“Actually we were looking of how to maximise the investment. Because actually nothing comes out of this thing, in meeting the [requirements from the] regulators.” (001)

As can be clearly noticed from the above two statements, it is interesting to note that the notion on maximising the investment and obtaining potential business benefits from a regulatory driven IT system implementation were mentioned by this particular interviewee, which came from the Compliance department. The statements have been made even though the interviewee was fully aware about accepted nature of compliance systems’ investments, in which they are not expected in any way to offer direct benefit banking business.

A similar sentiment to the above the notion of leveraging regulatory information to aid business is also being shared by another member of staff in the Compliance department. In this regard, the Head of AML/CFT and Compliance Strategy had suggested that irregular customer transactions which have been found to be legitimate, should indeed be leveraged for business:42

“If let’s say this customer’s transactions, maybe probably we classify under high net worth customer, and they are clean. The risk profiling shows that they

---

42 Please note that this interview statement has been first quoted in Section 7.2.2. It is being reproduced in this section for ease of reference, as well as to provide clear support to the discussion.
are low, you know, in terms of risk. So I suppose business should leverage these customers to do their selling... marketing...” (034)

It is critical to note that the idea of leveraging AML/CFT efforts to benefit business was not only confined to the Compliance department. As initially explained in an earlier section, it is highly fascinating to discover that even the President and CEO of Bank A is considered to be receptive to the notion of leveraging regulatory information to aid and benefit business. In this regard, Bank A’s President and CEO had specifically highlighted the opportunity to cross-sell to customers that have been risk categorised according to the AML/CFT requirements [see Section 7.2.2].

In the effort to further appreciate the distinctiveness of Bank A’s Compliance department’s interviewees being more open to the idea of leveraging regulatory information for business purposes, it was discovered that this unique standpoint can be attributed to the Compliance department’s tagline, which promotes the atmosphere of “Compliance Complementing Business”. The Head of Analytics was keen to provide assistance and support to other departments, and desired it to be viewed as a reference point for business, especially pertaining to regulatory matters:

“We are contributing, I would say. As the tagline goes, Compliance Complementing Business. We are now the reference point for business. As and when they have doubt for either a regulatory matter, things like ECM, BAFIA, etc. The businesses are aware that we are here to help and we make sure that we respond accordingly.” (017)

In a similar vein, the Head of AML/CFT and Compliance Strategy was of the opinion on the unique approach adopted by Compliance department towards business. In this regard, the interview had explicitly mentioned about the spirit of complementing business, and wishes the business to further leverage the department:

“Because probably our spirit. We want to complement business. We have an open concept where we want business to leverage on us. The information, the system that we have in place, that they can actually ride on us, so that we can pass back to them and for them to feel comfortable that they are doing with the right party.” (034)
Furthermore, the openness of Compliance department to the notion of leveraging regulatory information to aid business can also be partly credited to the Bank A’s “management thinking” shown during an assessment process for the feasibility of investment for the RSA2 system. In this regard, although customary justifications process was not stringently applied to a regulatory driven IT investment proposal due to the priority to be in compliant, the Head of Analytics had revealed that the rationale for establishing the new RSA2 system was somewhat being questioned by the superiors during what was known as a “challenge session”:

“You be surprised during the challenge session, they called it, where we present the paper, one of the bosses had asked us – so how much is the fine? Is it worth it to pay that amount [i.e. to be spent on the system] or pay the fine? ..... So when they were presented like savings in terms of cost, reports at the branches that we will be able to reduce... so all that we put a dollar value then only we can justify the investment.” (001)

The above situation presents an example where Bank A’s Compliance department was somehow being required to think about the possible benefits or savings that could be achieved through implementing a regulatory driven IT system. Hence, this situation can also be regarded as one of the likely underlying reasons that had contributed to the level of Compliance department’s awareness on the potential benefits that can be gained by AML/CFT IT system implementation. Furthermore, it is interesting to note that the situation has occurred even though the functions of Compliance department can generally be viewed as being independent, i.e. without being pressured to meet business targets and enhance business profits, as highlighted by Bank A’s Head of Integrated Risk Management:

“Because they [the Compliance department] are independent. They are very independent party and they are not really under pressure by business.” (037)

Having said the above, it is important and critical to reemphasise at this juncture that regardless of the aforementioned supplementary benefit pursuing activities, control aspects and compliance oriented efforts are still the main priority to Bank A’s Compliance department. This is probably the best way of explaining the situation as
to why this supplementary benefit has yet to be fully implemented, as part of its structured and established organisational business practices. As related by the Head of AML/CFT and Compliance Strategy, the main concerns of the department still remains as intending “to satisfy the regulator” and “more on the control aspects” (034). Therefore, the main driver for the organisation will continue to ensure the full and efficient deployment of the AML/CFT IT system, before other considerations could be incorporated.

The criticality of firstly meeting regulatory requirements is also shared by an interviewee from another organisation. As highlighted by an Executive Director from a local banking institution, regulatory compliance is extremely important for the organisation to implement and must be given the highest priority:

“Compliance to whatever regulations by authorities is utmost important to us. That’s I think is the overall, in terms of answer to the question, you know, where we stand in terms of compliance, is number one.” (026)

A second factor that influenced Bank A to possibly leverage AML/CFT false alerts can be appreciated through the IT infrastructure linkage that has already been established between its AML/CFT IT repository for RSA1 and the CRM1 system owned by the CRM department [see Section 7.5.1]. In this regard, Bank A can be considered as already having implemented established and structured organisational practices of leveraging AML/CFT regulatory information to aid the business, through this existing connection. In addition, once the future RSA2 system is fully operational and the RSA1 system is eventually decommissioned, a re-evaluation process on the strategy to leverage regulatory IT repository will eventually need to be carried out by the CRM department. As suggested by the Head of CRM, this reassessment process will likely initiate a review on the functionalities, capabilities and outputs of the new system to evaluate the possibility of using the new information made available by the system:

“When it replaces the current system, when we source our data, the IT technical staff will say that, ok now this is the new platform. And with this new platform, these are the new functionalities or the new capabilities, of the
output that the platform is providing. And from there itself we will do our analysis to see the potential of how to use this new information.” (024)

It is critical to note as well at this juncture regarding the assurance from the Compliance department pertaining the continuous support to be given to the CRM department, once the RSA2 system is in operation. The following statement was made by the Head of AML/CFT and Compliance Strategy, when asked about the future status of the RSA1 system, and its usage to the CRM department:

“Yes, [the RSA1 will be] shutdown. But we will continue to support CRM from the same angle.” (034)

Therefore, Bank A has already established an organisational practice of formally leveraging AML/CFT regulatory information to aid the business through the existing infrastructure linkage. In this regard, it is highly likely that the re-evaluation process mentioned by the Head of CRM will introduce further opportunities for the CRM department to leverage compliance information from the RSA2 system, as part of its structured and established organisational business practices. This situation can be attributed to the CRM department’s appreciation on the existing formal arrangement of accessing the AML/CFT IT repository for business purposes.

To further reinforce the above possibility, it may be interesting to appreciate that Bank A’s event-based marketing initiatives have indeed generated a huge amount of new sales for the organisation since the programme was initiated. As revealed by one of Bank A’s internal document that was made available to the researcher, for a period of about three years since the deployment of the programme, the organisation was able to obtain an astonishingly “RM 3 billion in new sales” [D018, p. 4]

It is nevertheless sensible to argue that the percentage contributed by the decision to leverage the AML/CFT IT repository in attaining the huge amount of new sales could not be accounted for with absolute certainty. Nevertheless, since the IT repository is considered as one of the main informational input to the CRM1 system [see Section 7.5.1], the important role played by the regulatory data in contributing to the achievement of this significant success should not be ignored. Briefly reiterating the discussions presented in various earlier sections of this chapter, the regulatory IT
Chapter 7: Analysis of Supplementary Benefits

repository had indeed given the CRM department an opportunity to obtain comprehensive customer transactional information that had been cleansed and in a consistent and coherent formatting. This has further facilitated CRM efforts in uncovering irregular transactional patterns, which in turn could trigger event-based marketing initiatives which had benefited the organisation through the RM 3 billion of new sales mentioned earlier. Moreover, the opportunity to leverage the regulatory IT repository had also enabled cost effective and speedier operations for the department, as opposed to sourcing the needed information directly from the core banking system and various other fragmented systems in Bank A.

Therefore, all the above had demonstrated the criticality of information sourced from a system being established for regulatory purposes in order to enhance the capabilities of CRM department in implementing event-based marketing initiatives in Bank A. Additionally, it has also presented the criticality for this department to continue accessing RSA2 central repository upon the discontinuation of the RSA1 system. Therefore, through an inevitable re-evaluation process arising from the new AML/CFT IT system, it is may be highly likely for the CRM department to experience the supplementary benefit of leveraging AML/CFT false alerts, as part of its structured and established organisational business practices.

**Thirdly, and finally,** there is an *existing formal practice* adopted by the CRM department that can also be regarded as one of the reasons to allow Bank A to plausibly leverage AML/CFT false alerts as part of its established business process. It was discovered that there was a common procedure to utilise an output from another regulatory related system when evaluating the feasibility of marketing leads generated by its CRM1 system.

As acknowledged by the Head of CRM, all generated marketing leads will be compared against the information in Bank A’s internal CCRIS\(^43\) database. This database is a repository that provides credit worthiness information on customers based on their

\(^{43}\) The Central Credit Reference Information System (CCRIS) is an IT database maintained by the central bank, which contains detailed credit information of borrowers in Malaysia. However, as mentioned in the above sentence, the term CCRIS in this context is actually referring to Bank A’s internal database, which happened to be utilising a similar acronym, as well as having a similar nature of information.
borrowing history, such as whether they are categorised under non-performing loan (NPL) or otherwise. The following two statements made by this interviewee had provided insights into how the information from the internal CCRIS regulatory database had been utilised:

“..... so let’s say we are able to identify 5,000 customers who have deposit accounts with us, they are our profitable customers and yet they pay loans elsewhere. So now, before we can even prospect them, we need to know whether they are good or not.” (024)

“So what we do is that, with these names, we will go to the CCRIS records and check. I mean the CCRIS record at Bank A’s side, not at Bank Negara [i.e. the central bank]. So we check here, ok we see, oh, this guy is good. He has made good payments and all, so basically he passed some of the risk quality information.” (024)

Arising from the above explanations, the records residing in the internal CCRIS database are being used by the CRM department to act as one of the reference point in allowing customer feasibility to be initially verified. This situation is particularly useful especially in the case where marketing leads generated by the CRM1 system need to be checked for viability.

Therefore, having appreciated this existing practice of utilising CCRIS regulatory information as a reference for evaluating the feasibility of marketing leads generated by its CRM1 system, it can therefore be safely mentioned that a similar perspective might likely be occurring with Bank A’s AML/CFT IT system. In this regard, it can be assumed that it might not be highly unusual if the CRM department had decided to leverage the output from the RSA2 system. This situation can be further made possible arising from the re-evaluation process that need to conducted due to the implementation of the RSA2 system, as mentioned in an earlier discussion.

In effect, it is essential to note that Bank A’s CRM department was indeed under the impression that they have already leveraging the output from the organisation’s AML/CFT system. In this regard, interviewees from the CRM department were having the notion that all information obtained from the regulatory IT repository (i.e. as
Chapter 7: Analysis of Supplementary Benefits

described in Section 7.5.1) had already excluded the list of customers that were
deemed related to ML/TF. For example, during an interview with the Head of CRM,
the interviewee had highlighted about the filtered information that the CRM
department was accessing:

“So those customers, you see, they have actually been filtered. Ok these are
the bad customers so called who are in anti-money laundering. So this list of
customers will not be our hot list. So we will always exclude these customers
from prospecting.” (024)

In addition, the same interviewee had even acknowledged that the department will
not be having the opportunity to access these filtered customers information if
information is to be extracted directly from the various source systems in the
organisation:

“So for us, we take it from here, mainly because it has already been filtered.
The bad account and all those, have been filtered. So that was the reason. If
we go straight to the source systems, we will miss this filter.” (024).

However, as had already been explained earlier [see Section 7.5.1], it needs to be
noted that the information being accessed by the CRM department was effectively the
raw and unprocessed (albeit cleansed) transactional data. Therefore it contains no
information from the output from the AML/CFT IT system, as well as having
undergone any filtration process.

Nevertheless, it is interesting to note on CRM interviewees’ awareness and
appreciation on the benefit of leveraging AML/CFT information. Therefore, this
particular awareness (as well as incorrect interpretations) by the CRM department can
thus be importantly considered as another justifying factor to support the earlier
statement. In this regard, it might not be surprising if the department had decided to
leverage the output from the RSA2 system. This is arising from the department’s firm
appreciation on the value that could be derived from the implementation of an
AML/CFT IT system.
Chapter 7: Analysis of Supplementary Benefits

c) Bank B

For the case of Bank B, outcome from the analysis of interview data seemed to suggest that the organisation can be regarded as having no tendency to experience this supplementary benefit, or even considering achieving the benefit as part of its future strategy. The situation within Bank B is because there is less evidence to suggest that interviewees from this organisation were being receptive to the notion of leveraging regulatory information for business purposes. The discussions that follow will justify this assertion in detail, by outlining the insights from various interviewees from Bank B that have indeed pointed towards this situation.

For example, the bank’s Director of Consumer Bank Risk Monitoring was of the opinion that AML/CFT false positive alerts could not possibly provide any business benefits to the organisation. The interviewee was of the view that cross-selling activities based on false alerts will provide inadequate information:

“But you see, I don’t know whether they have adequate information or not in the system. Because the system will throw alerts. They only working on the alerts, you know.” (025)

“So even if they want to cross selling, you can only cross-sell [using] those alerts.” (025)

Having said the above, it is interesting to note that the same interviewee had also acknowledged that AML/CFT exception reports used prior to the implementation of RSB1 system had indeed been used by Bank B’s branches for sales purposes in the past. In this regard, it was made known to the researcher that previous exception reports were extracted from the core banking system on periodic basis, and produced for branches to review:

“Hmm... ok... maybe not so often, they [the branches] said that they can also... other people can actually use that... not RSB1... earlier, you know we had that core banking system reporting... so they used that one for sales purposes.” (025)
Chapter 7: Analysis of Supplementary Benefits

This has prompted the researcher to probe further aiming to appreciate the possible reasons as to why similar information was not being extended when the RSB1 system was established. The interviewee had, in response, stressed that the RSB1 was dedicatedly built for the purpose of AML/CFT. Therefore, it is said that the branches were not expecting that the system would serve other possible purposes:

“... because the RSB1 is a dedicated system, so it may not... you know... be throwing out such information for them to [use].” (025)

A sentiment similar to the above could also be sensed from other interviewees in Bank B. For example, during an interview with a Project Manager from the Transformation Office (whom was previously overseeing the implementation of RSB1), the interviewee had highlighted that other objectives were not being considered during the development of RSB1. This approach was adopted in order to ensure that the project was focusing exactly on its original intention:

“The system must be very focused... what exactly we wanted to do. The scope of the application or system that we want to do must be sensible enough that the return of investment does make sense for us to do this [i.e. to incorporate other objectives].” (042)

In addition, the same interviewee had also considered that the AML/CFT IT system in Bank B as already been successfully implemented. This was due to the fact that the system had accomplished what it was originally set out to achieve, and thus no further changes should be made:

“I would say the AML system that we have right now, I know it sounds selfish, it’s perfect already. I think what was set out to achieve, it has got that.” (042)

Having said this, it may be worth reiterating that this interviewee was, from the Transformation Office of Bank B. Among others, the function of Transformation Office was said to facilitate the maximisation of returns on investment from IT systems implemented in the organisation. This is to be achieved by way of including other user groups' interests that could similarly benefit from any IT systems being implemented. When describing the functions of Bank B’s Transformation Office, the same interviewee had indeed highlighted the notion of “leveraging on each other”, to
ensure no duplication of efforts, as well as to achieve greater good by avoiding efforts that only “provide returns to a specific group of people” (042). Nevertheless, as it may be noted from this sentiment, it can be concluded that the effort to leverage AML/CFT IT system to possibly benefit other departments besides Compliance was not considered as part of the overall agenda.

Moving to the insights obtained from another interview with the AVP from Bank B’s IT department, the interviewee had emphasised that the logic used in an AML/CFT IT system differs from a system used for business analytics. Therefore, this interviewee was of the opinion that these systems should be leveraged or tapped separately for distinct purposes as they are looking from different viewpoints altogether:

“Actually I believe AML should be tapped separately. Whereas in terms of the cross-selling has a different logic altogether.” (040)

In a similar vein, interviewees from Bank B’s business departments that are responsible for customer analytics are also echoing the same sentiment highlighted in the preceding paragraphs. Both the Head of Retail Banking and the Head of Preferred Banking have generally similar opinion regarding the overall motivation for establishing the compliance function, which they felt was never intended to enhance the organisation’s business. As related by the Bank B’s Head of Retail Banking, while compliance is regarded as absolutely necessary, it is however not a money generating function of the organisation:

“It [i.e. compliance] is a necessary thing, especially in the banking environment, where we’re handling people’s money. But let’s be real, compliance is not going to make us extra money.” (039)

Furthermore, Bank B’s Head of Preferred Banking had clearly articulated that it is not the compliance function’s role to directly enhance business. The interviewee had made the following two comments when asked whether there were any instances where the compliance function had directly enhanced banking business:

“No. That one I can say. It’s clear. Not their role. Don’t blame them, it’s not their role.” (041)
Chapter 7: Analysis of Supplementary Benefits

“And if Compliance start enhancing the business, then you’ll also worry, they’re getting your job.” (041)

Therefore, compliance function in itself is not expected to generate any returns for the organisation and it would be even typical or common to consider compliance role to be against business due to its contradictory objectives. Moreover, it is interesting to note that the Head of Preferred Banking is subscribing to the “old school thinking”, which had advocated the segregation between marketing and compliance roles, since these two very important sides of business were said to be different in nature and hence, should be kept separated. This interviewee had shared the above opinion during the interview when asked if any processes or outputs from the AML/CFT IT system can be benefited by the marketing side of the organisation:

“Marketing side... hmm... maybe I’m a bit old school, I would like to see some separation between two very important sides of the business.” (041)

A slightly more favourable impression was detected in a separate interview with Bank B’s Head of Group Compliance. As shown in the following interview statements, the interviewee had specifically suggested that compliance role in the banking group should be regarded as a function that does not hinder business. The interviewee was also of the opinion that compliance should be achieved through obtaining buy-in from business departments after they have been made fully aware of all the possible compliance risks that will result from actions that they are intending to undertake:

“Ok, buy-in here means you must be able to explain to the business that you are not here to thwart their activities, you’re not here to hinder them from doing what they want to do, you’re not here to be a road block. We need to be seen as a facilitator. If we have had that, then the buy-in is there. So when we tell them that this is something that you want to do, and it’s going to be very risky, they are willing to listen.” (007)

However, it may be worth noting that this obtaining buy-in approach mentioned by this interviewee is not from the perspective of directly benefiting business. Instead, it can be viewed from the general standpoint of educating the relevant stakeholders accordingly, in order to avoid the associated cost of non-compliance. Hence, the
overall approach advocated by Bank B Group’s compliance function can also be regarded as one of the reasons why Bank B’s Compliance department is seen to be deploying its AML/CFT initiatives without ever considering any potential business benefits that could be leveraged by other departments.

Therefore, having presented the above views of Bank B’s interviewees, it can safely be assumed that Bank B’s is lacking any clear motivation to seek the supplementary benefit of leveraging false AML/CFT alerts to directly benefit banking business. This assertion is also primarily based on the understanding that Bank B is seen to be lacking in the likelihood of reaching a stage where the suggested supplementary benefit would be achieved through structured and established organisations practices.

In summary, supplementary benefit arising from the opportunity to leverage time-critical and event-based information to directly benefit banking business can therefore be achieved through the implementation of AML/CFT efforts within the organisation. Nevertheless, it is worth noting that this type of supplementary benefit is more inclined to be experienced by Bank A, arising from the extensive explanation provided. Therefore, the above discussions have sufficiently elaborated the realisation of this particular supplementary benefit, through the rationalisation provided, as well as the appreciation on the associated requirements and insights from the interviewees. Table 7-6 provides a structured summary to the above discussions, pertaining to this specific supplementary benefit by appreciating the situation specifically for Bank A:

<table>
<thead>
<tr>
<th>Factor</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>What</td>
<td>• What is the description of the supplementary benefit?</td>
<td>• Opportunity to timely detect and leverage selected customers’ transactional activities that are found to be unrelated to ML/TF activities, and consequently be used as an input to the organisation’s business relationship enhancement activities. By doing so, organisations will also be able to directly reduce the risk of inadvertently engaging with customers that may be associated ML/TF activities.</td>
</tr>
</tbody>
</table>
## Chapter 7: Analysis of Supplementary Benefits

<table>
<thead>
<tr>
<th>Factor</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Why</td>
<td>Why is the supplementary benefit feasible?</td>
<td>The supplementary benefit is feasible as false alerts can also be regarded as customers’ genuine financial activities that have gone beyond their common financial activities and behaviours. Therefore, they may represent specific instances of a customer’s needs and wants, and therefore signify the possibility of deploying time-critical event-based marketing initiatives. Furthermore, coupled with the strengths of computerisation, these initiatives would be more appealing due to the associated higher efficiencies.</td>
</tr>
<tr>
<td>Where</td>
<td>Where is the supplementary benefit arising?</td>
<td>The supplementary benefit will arise from the utilisation of AML/CFT false positive alerts within the organisation’s marketing efforts.</td>
</tr>
<tr>
<td>When</td>
<td>When will the supplementary benefit be realised?</td>
<td>The supplementary benefit will be realised subsequent to the generation of the AML/CFT alerts and the review process that follows.</td>
</tr>
<tr>
<td>Who</td>
<td>Who (or which party) will have access to the supplementary benefit?</td>
<td>The CRM department (with permission) will have access to the supplementary benefit.</td>
</tr>
<tr>
<td>How</td>
<td>How will the supplementary benefit be made available?</td>
<td>The supplementary benefit will be made available electronically through the generation of the alerts, as well as manually through the subsequent enhanced CDD process.</td>
</tr>
<tr>
<td></td>
<td>How useful is the supplementary benefit in contrast to alternative benefits?</td>
<td>The supplementary benefit is useful and critical, as it would be able to initiate marketing initiatives that leverage specific incidences of a customer’s needs or demands. In addition, since is uniquely associated with AML/CFT false positive alerts, similar benefit is not available in other types of exception reporting or flagging mechanisms employed by the organisation.</td>
</tr>
</tbody>
</table>

### 7.7. CONCLUDING REMARKS

In conclusion, this chapter has outlined the supplementary benefits from the sample organisations’ activities that are considered to be beyond simply meeting regulatory requirements, and seen to be directly and positively impacting the performance of banking institutions. The presentation on analysis of supplementary benefits is critical to this research, as it has provided useful insights into the various opportunities that can indeed be beneficial to organisations, arising from the implementation of regulatory driven AML/CFT IT systems. However, it may also be useful to appreciate that in a highly inter-connected IT environment, benefits often emerged from complicated interactions between numerous IT systems and business processes.
(Doherty, 2013). Therefore, they may not necessarily arise solely from the direct implementation of any single IT system. The same principle can indeed be applied to regulatory IT systems, in which the identified supplementary benefits presented earlier had, in effect, emerged from the needed interactions with other systems to obtain the necessary information. Furthermore, the required supplementary activities arising from the information or alerts generated, as well as the linkage with another system leveraging information being made available had also resulted in the realisation of benefits.

Moving forward, having appreciated both types of benefits that have been identified by this research, it is also critical gain understanding on the diverse IT and non-IT capabilities that have been regarded to have facilitated, to a certain extent, the attainment of these two benefits. In this regard, presentation on the analysis of capabilities will be elaborated in detailed in the subsequent Chapter 8.
8.1. INTRODUCTION

This chapter will proceed to present the final detailed analysis for the thesis. In this regard, it will be addressing two research objectives that have been previously highlighted in Chapter 3 (i.e. RO3 and RO4). Research objective RO3 is aiming to explore and understand the portfolio of IS capabilities that have assisted banking institutions in attaining expected compliance benefits, as well as those that have facilitated the achievement of supplementary benefits. Meanwhile, RO4 is also investigating how through the utilisation of these capabilities in accomplishing these two types of benefits, a financial institution might improve its competitive positioning.

It is acknowledged that up to this point, the discussion on compliance and supplementary benefits have been the prevailing theme, as compared to the explanation of associated capabilities. While it is not implying any lesser importance, it needs to be appreciated that the discussion on the relevant capabilities would not be meaningful if both benefits had yet to be elaborated and discussed in detail. Hence, it is envisaged that only by possessing deep understanding of these benefits, will the situation allow for any meaningful discussion of the various capabilities that have been considered to influence or facilitate the attainment of these benefits.

In achieving the above intention, this chapter will be presented according to the following structure. It will start by highlighting the analytical approach undertaken during the analysis of capabilities. In addition, the analysis on capabilities that have been regarded to be influencing the achievement of compliance benefits will then be discussed in detail. Similarly, a comprehensive discussion on capabilities that are seen to be contributing to the accomplishment of supplementary benefits will then be
presented. Furthermore, the presentation on capabilities will also be discussed from the perspective of organisation’s competitive positioning. Finally, the concluding remarks section will summarise the findings of this chapter.

8.1.1. Analytical Approach

In similar perspective to previous analysis chapters, although the broad analytical approach has been articulated in Section 5.4.5(b), it is important to add the following qualifiers, which explain how the approach has been applied to capabilities. In addition, specific approaches adopted for each type of benefits will also be available, and they will be presented within their own respective sections [see Sections 8.2.1 and 8.3.1]. The identified capabilities were mainly derived from the interview data, and subsequently contrasted with the list of capabilities, suggested in Section 3.4.2. It is important to note that the rationalisation on identified capabilities have also significantly capitalised on the extensive discussion and understanding obtained from the last two chapters.

Nevertheless, this analysis will still be predominantly substantiated by relevant interview quotes, where available, in order to strengthen the rationalisation provided for each identified capabilities. In a similar approach to the previous analysis chapters, excerpts from interviews related to Bank A and B will primarily be used to provide insights and understanding on the identified capabilities. However, perspectives from other organisations, inclusive of the regulatory authority, will likewise be taken into account as well. This specific approach was adopted with the aim to obtain further explanations and supporting justifications, as well as to explore alternative viewpoints in the effort to explain the circumstances that are uniquely affecting these detailed case study organisations.

Moving the discussion on the presentation of capabilities, it needs to be noted that there are several extra capabilities that have been discovered arising from the analysis of the interview data. In this regard, these extra capabilities have been classified as additional capabilities, since they are not part of the list of key capabilities originally
Chapter 8: Analysis of Capabilities

suggested by Wade and Hulland (2004). Accordingly, the suggested definition for each type of these additional capabilities will be provided, together with the rationale for the importance of their role in achieving potential benefits for the organisation.

In addition, as briefly highlighted in Section 3.4.2, it is useful to explain the utilisation of these capabilities and their relationship with the attainment of compliance and business benefits, specifically from the perspective of IT function. However, this research will also be presenting the employment of similar capabilities by other functions within the organisation, in particular, from the viewpoint of the Compliance department. This approach can be attributed to the understanding that the implementation AML/CFT IT system is primarily driven by regulatory requirements. Therefore, since they will be mainly managed or overseen by the Compliance departments of these organisations, some of the capabilities being discussed in this chapter have been regarded as instead being more inclined to be utilised by this particular department.

8.2. CAPABILITIES FOR COMPLIANCE BENEFITS

8.2.1. Overview and Specific Approach

In general, most of the capabilities suggested in Chapter 3 have been discovered in the two detailed case study organisations in one way or another, i.e. being utilised within the organisational efforts to meet regulatory requirements. However, it is worth noting that the usage of these capabilities may not necessarily be limited to the development of AML/CFT IT system per se, but can also be applicable to the overall efforts of implementing the AML/CFT initiatives within the organisations. Therefore, the identified capabilities in this section can also be regarded as being *commonly utilised* to fundamentally establish and deploy AML/CFT efforts in the organisation and avoid the possible penalties from the regulatory authority.

In specific relation to the analysis of capabilities on compliance benefits, the research had further adhered to the following approach:
i). The analysis assumes that all capabilities exhibited by the detailed case study organisations have facilitated the accomplishment of compliance benefits. Since organisations are attempting to comply with the regulatory requirements on AML/CFT being imposed upon them, all the capabilities that have been utilised to meet the expected deliverables can therefore be directly associated with the aim to achieve compliance benefits. This statement can be depicted by the dotted line in the lower portion of the following Figure 8-1:

![Figure 8-1: Capabilities Associated with Compliance Benefits](image)

ii). The analysis aimed to uncover and appreciate the capabilities that are associated with compliance benefits in general. Therefore, the effort will primarily be focusing on identifying these capabilities, as well as understanding their relevance to an organisation’s efforts to comply with AML/CFT requirements. Importantly, it will be done without further attempting to establish the exact nature of relationship between each specific capability and a particular compliance benefit identified in Chapter 6. As illustrated by Figure 8-2 below, all capabilities are generally assumed to have influenced each and every compliance benefit that have been identified, and thus ignoring specific and distinct relationships that may possibly exists between them.

![Figure 8-2: General Relationships - Capabilities and Compliance Benefits](image)
The above decision arises from the understanding that all related organisations within the industry are expected to be fully compliant with the AML/CFT requirements. Since the expected regulatory deliverables are regarded to be similar, therefore, the associated compliance benefits should not be uniquely experienced by any particular organisation. This approach can also be seen as in harmony with the institutional theory, in which proposes that when responding to external pressure (such as compliance) different firms will tend to react in similar ways (Krell et al., 2011). Hence, it would be less interesting to appreciate the differences in capabilities being used to achieve each compliance benefit that would commonly be experienced by each banking institution anyway. This particular situation should be contrasted with the criticality to recognise and identify these capabilities, which need be treated as the set of key capabilities that are significantly required when complying with AML/CFT requirements. Therefore, the nature of relationships between these capabilities and the various outcomes may not be an area of research that worth to be explored in detail;

iii). The analysis also did not attempt to compare and contrast the capabilities exhibited between Bank A and B, as well as the ones highlighted by the interviewees from the regulatory authority and other banking institutions that the researcher were managed to gain access to. The identified capabilities were rather presented in a summarised and aggregated approach, cutting across all the organisations where the interviews were conducted. This is in line with the approach presented in the preceding paragraphs;

iv). The research has sought to ascertain at which stage of the AML/CFT implementation efforts the capabilities will be playing their most significant role. In this regard, the stages identified are either in the midst of establishing the regulatory driven IT solution (i.e. the pre-deployment stage), or subsequent to its complete and successful implementation (i.e. post-establishment). It is sensible to argue that most of the capabilities being presented in this chapter can somehow

44 However, in contrast, the nature of relationship between selected capabilities and the identified supplementary benefits will indeed be established in Section 8.3, due to their appealing possibility in uniquely influencing the institution’s competitive positioning.
be useful in any or all of the stages in the implementation. Nevertheless, it would be more meaningful if the capabilities can be explicitly distinguished in phases that they will be regarded as most useful or consistently playing a critical role. Similarly, the analysis will also be identifying which department (i.e. especially Compliance or IT departments) that has been seen to be most actively utilising the capability to meet regulatory requirements, and therefore achieving compliance benefits.

The rest of the presentation in this section will continue to discuss each capability, explaining its role in facilitating the attainment of compliance benefits. The discussion will first be presenting the capabilities according to the classification suggested by Wade and Hulland (2004) [see Section 3.4.2]. In addition, a separate presentation will also be conducted on the identified additional capabilities.

Importantly, the presentation for each capability under this section will tend to meet the following sequence of presentation. It will typically start by providing the definition of the capability, as well as the rationale of its significance. Where available, relevant interview quotes expressing the views and opinions of the research participants will also be presented in order to offer richer explanations. This is then followed by an analysis of the department that has been regarded as having typically utilised the capability, and therefore achieved compliance benefits. Finally, the stage (i.e. either the pre-deployment; or post-establishment stages) where the capability is considered to be most useful or consistently play a critical role will also be identified.

8.2.2. Outside-in Capabilities

Outside-in capabilities are the type of capabilities that are regarded to be externally focused. They are used to anticipate market requirements, understand organisational rivals, and establish customer relationships that are long-lasting. The capabilities that have been categorised under this type are External Relationship Management (ERM); and Market Responsiveness (MR). Their roles in influencing and assisting the attainment of compliance benefits through the deployment of AML/CFT activities within the organisation are explained in the following sections.
a) **External Relationship Management (ERM)**

From the context of regulatory compliance, the ERM capability is *defined* as the: 

“ability to manage relationships with external stakeholders, where necessary assistance, cooperation and information are required to be obtained in order to facilitate effective regulatory compliance.”

As shown in the upper portion of Figure 8-3, the key external stakeholders for AML/CFT implementation are regarded as the regulatory authority, and the AML/CFT software and hardware vendors. Interactions with the regulatory authority are typically concentrated on AML/CFT implementation issues, which generally focus on understanding the requirements and obtaining further clarification. On the other hand, interactions with the software and hardware vendors are generally concentrated on the efforts to implement an AML/CFT IT solution, as well as to appreciate software vendor’s best practices based on their expertise and previous experience. Therefore, the capability to obtain guidance and clarification from the regulatory authority; as well as to achieve cooperation and ability to leverage vendor’s expertise and experience; can be regarded as one of the important inputs to ensure smooth deployment of AML/CFT related activities within the organisation.

**Figure 8-3: Key Stakeholders in the AML/CFT Implementation**

Based upon the above explanations, it is possible to hypothesise that the ERM capability would typically be required for implementing AML/CFT initiatives. This is premised upon the general understanding that the various needed interactions
mentioned earlier would typically and normally be required in any instances of regulatory driven initiatives involving the establishment of IT systems, and thus should not only be confined to implementation of AML/CFT efforts.

In relation to the views and opinions of research participants, several interviewees have indeed highlighted the need to interact with the external stakeholders, in order to facilitate their implementation of AML/CFT. For example, Bank A’s Head of Analytics had explicitly mentioned the need to constantly and continuously interact with the hardware and software vendors, during the implementation of RSA2 system:

“With the new [RSA2] project, you have to interact a lot [i.e. with the vendors], to understand their limitations ..... So interaction is very critical, for example the delivery of hardware, must be on schedule.” (002)

Similar sentiment can also be detected in Bank B. In this regard, the Vice President for Consumer Bank Risk Monitoring had mentioned about the high level of engagement between the organisation and the AML/CFT IT vendor:

“There’s a lot of engagement with the vendor ..... in fact just now the text [on the phone] was from the vendor. So there’s a lot of engagement.” (006)

Viewed from the perspective of obtaining the vendor’s best practices and leveraging their expertise and experience, Bank A’s Head of Analytics had highlighted the extra benefits provided by the software vendor to implement the AML/CFT IT solution:

“And the vendor had also bring the best practices, what are other banks are using.” (001)

In addition, in a separate interview with Bank A’s IT Department lead for the RSA2 system, the interviewee had similarly echoed the sentiment about the software vendor valuable guidance and advice:

“...this vendor has [provided] the value-add of advising us – ok maybe you shouldn’t implement this one ..... maybe you should take another scenario, which can meet your minimum requirements as well as extract a few other things.” (004)
Moving the discussion to the perspective of the interactions with the regulatory authority, Bank A’s Head of AML/CFT and Compliance Strategy had highlighted the typical interactions with one of the departments in the central bank, i.e. the Financial Intelligence Unit (FIU)\textsuperscript{45}. In this regard, the interview had explicitly mentioned the discussion with FIU prior to the issuance of the AML/CFT guidelines. Therefore, this discussion session can be regarded as one of the avenues for the Compliance department to obtain further clarification:

“The FIU actually called us for, you know, when they come up with the draft guidelines. They actually call us for discussions, feedbacks” (003)

The importance of interacting with the regulatory authority was also supported by an interviewee from Bank B. In this regard, the Vice President for Consumer Bank Risk Monitoring had mentioned the interactions with FIU, prior to the AML/CFT guidelines being issued to the industry:

“In fact before Bank Negara [i.e. the central bank] came out with the guidelines, there were a lot of engagement, between FIU and ourselves, bankers.” (006)

In addition to providing feedbacks, interactions with the regulatory authority were required during the implementation of AML/CFT IT systems. As related by the IT Department lead for the RSA2 system, there was an instance where direction from the regulatory authority was sought:

“And at that point of time I would say, we were also in discussion with Bank Negara [i.e. the central bank], to see, I mean those requirements whether we can further explore, how best to meet those set of items.” (004)

Therefore, arising from the above discussions, the ERM capability seemed to have the tendency to be utilised by both the Compliance and IT departments. In addition, it is regarded to be most useful or consistently playing a critical role during the pre-deployment stage of the AML/CFT IT solution. In this regard, the capability is regarded as being continuously needed when organisations are in the midst of establishing their

\textsuperscript{45} The Financial Intelligence Unit (FIU) is a department within the central bank that, among others, oversees the submission of AML/CFT exception reporting by relevant institutions in Malaysia. It is also responsible to liaise with other regulatory authorities when further investigations or actions are required, which includes prosecutions in the court of law.
AML/CFT IT solutions, as well as during the effort to discuss and appreciate new regulatory requirements prior to the actual implementation.

The above situation can further be contrasted with the *alternative stage* (i.e. post-establishment). In this particular stage, it can be regarded that managing relationships with related external stakeholders would be less important and most likely to be done on an occasional basis when the AML/CFT initiatives have been fully and successfully implemented. For instance, whenever any minor system changes need to be carried out, such as due to additional regulatory requirements and further fine-tuning, they can be considered as an ad-hoc activity.

b) **Market Responsiveness (MR)**

The MR capability from the perspective of regulatory compliance is *defined* as the: “*ability to collect and disseminate information (i.e. including pertaining to threats and opportunities) obtained from external sources, and accordingly responds to any regulatory changes.*”

This particular capability can be regarded as typically be required for AML/CFT deployment due to the need to ensure that ML/TF monitoring and detection processes within the organisation are efficient and up-to-date. Therefore, information obtained from various external sources is regarded as highly critical to achieve this aim. In this regard, the MR capability can be utilised to obtain new developments on ML/TF from subscriptions to and monitoring of online resources; and memberships with external entities or committees. In addition, it can also be achieved through obtaining latest developments from vendors; as well as appreciating any recent developments experienced by overseas branches.

In relation to the *views and opinions of research participants*, several interviewees have indeed highlighted the various avenues to obtain latest developments regarding AML/CFT mitigating efforts. In this regard, one Vice President had highlighted the activities adopted by his organisation, which include monitoring of related information via the Internet and through professional memberships:
“....there is a website that actually provides information on money laundering. We do [monitor] that. And then we have our colleague here who actually is a member of this fraud examiners. So he actually has a booklet that he receives, magazine that he receives every month is being analysed.” [006]

In relation to Bank A, the Head of Analytics had also highlighted the organisation’s subscriptions to external services that provide alerts to the organisation. The information obtained might then be used to devise the necessary counter measures:

“We have subscribed to a few you can called it... newsletter or on-line services, [to] provide these kinds of alerts. ..... [we] will be prompted when there are changes ..... we are more interested in their modus operandi. So the moment we understand how the perpetrators work, we start to design the counter measures.” (002)

In addition to subscribing to external services, external information can also be obtained through organisation’s membership to the Compliance Officers Networking Group (CONG). CONG committee members comprise of selected staff from the Compliance departments of banking institutions in Malaysia, as well as representatives from the regulatory authority. Meetings are conducted once a month, to discuss compliance related matters, which include new and emerging AML/CFT developments. Hence, it gave CONG members the ability to be responsive to any changes to the requirements that the regulatory authority is contemplating to put into effect.⁴⁶

In relation to CONG, Bank A’s Head of Analytics had specifically mentioned about the opportunity to obtain advance information pertaining to AML/CFT requirements through this committee:

“..... they have a committee called the Compliance Officers Networking Group, where all the commercial banks in Malaysia, their compliance departments

⁴⁶ Although it has been highlighted in the earlier Section 8.2.2(a) that discussions between banking institutions and the regulatory authority were available prior to the issuance of AML/CFT requirements, it is nevertheless worth to explicitly highlight these interactions through the CONG committee. This is based on the understanding that the CONG committee can be regarded as a more structured process and an established channel of discussion.
Chapter 8: Analysis of Capabilities

[representatives], actually meets every month. ..... They discuss new regulations, new laws that Bank Negara [i.e. the central bank] is proposing. ..... So we do get a heads up from Bank Negara.... unofficially.” (001)

The role of vendors in sharing latest market developments on AML/CFT was also noted through the interviews. It is acknowledged that this type of market developments information may not necessarily be directly related to any regulatory requirements. Nevertheless, by tapping on vendor’s capability to keep abreast with AML/CFT developments may act as one of the ways for organisations to critically build their awareness and subsequently respond to changes in the regulatory requirements, if any. In this regard, Bank A’s Head of Group Compliance had explicitly mentioned the role of the vendor in furnishing the latest trends on AML/CFT:

“.... this trend also will come from our vendor, the one who provides us the system, which they have committed that the latest trend of money laundering will be shared with all users, or those who had procured the [same] system.” (008)

Furthermore, another channel to forecast any potential updates to the AML/CFT requirements can be done through leveraging the institution’s overseas branches. As related by Bank A’s Head of Corporate Regulatory, by monitoring new developments affecting Bank A’s overseas branches, the information may indicate that similar requirements could eventually be implemented in Malaysia:

“These new developments are not particularly a surprise to us because we operate globally as well. So we have the opportunity of experiencing the new regulations and guidelines that are being in placed in New York, in London, in Hong Kong or Singapore for that matter ..... So it’s just a matter of time [for the new developments to arrive in Malaysia].” (009)

The MR capability can be regarded as having the tendency to be utilised by the Compliance department. In addition, it is also seen to be most useful or consistently playing a critical role during the post-establishment stage of the AML/CFT initiatives. This is premised on the understanding that Compliance department will need to constantly keep abreast with the latest developments, once the AML/CFT efforts have
been fully implemented. In addition, it will also need to promptly reflect any changes with a revised organisational monitoring and mitigating measures.

The above situation can further be contrasted with the pre-deployment stage. In this particular stage, it can be regarded that the MR capability would be less needed as the effort to mitigate the risk of ML/TF has yet to be established as part of the organisational practices. Therefore, it has yet to reach the stage where the latest developments on AML/CFT will need to be gathered and kept updated in a organisational established practices.

8.2.3. Inside-out Capabilities

Inside-out capabilities are the type of capabilities that are used to react to market requirements and opportunities. This type of capabilities is typically initiated from within the organisation and tends to be internally focused. The four capabilities that have been classified under this category are IS Infrastructure (ISI); IS Technical Skills (ISTS); IS Development (ISD); and Cost-Effective IS Operations (CEISO). The following sections will provide the discussion on how some of these capabilities have influenced or facilitated compliance benefits, arising from the deployment of AML/CFT initiatives within the organisation.

a) IS Infrastructure (ISI)

The ISI capability from the context of this research is defined as the: “ability to establish appropriate technological infrastructure that effectively facilitates compliance to regulatory requirements.”

In relation to the AML/CFT initiative, this capability facilitates the implementation of IT solutions that enable timely information, analysis, and detection of suspected ML/TF activities. As highlighted in Sections 6.5.1 and 7.5.1, the establishment of AML/CFT IT systems are considered as non-mandatory, but highly encouraged. Therefore, arising from this flexibility of implementation, the ISI capability can generally be regarded as not being typically required in deploying AML/CFT initiatives within the organisation.
Nevertheless, particularly for organisations having large number of banking customers, and with high volume of daily transactions, such as Bank A and B, the implementation of AML/CFT IT solutions may indeed be critical. This is further taking into consideration that deploying manual operations will not be entirely feasible in these two organisations. Especially in a situation when comprehensive drill down on customers’ accounts and other information are required arising from the need to conduct further investigations, manual operations will be considered as impractical.

In relation to the views and opinions of the research participants, it is worth mentioning that one interviewee had provided a sound argument for the significance of the ISI capability. In this regard, Bank A’s Head of Group Compliance had highlighted the organisation’s critical dependency on an IT system, due to the impracticality of implementing manual AML/CFT operations:

“Our supervision in terms of money laundering is highly depending on system, because of our nature of operations and volume that we transact daily is voluminous.” (008)

Therefore, appreciating the related discussions for Bank A and B in the last two chapters, it can be regarded that an IT solution would be highly critical in these organisations. Also, it is sensible to further argue that having the capability to enable the establishment of appropriate regulatory technological infrastructure in these two organisations would be similarly vital.

Consequently, it can further be regarded that the ISI capability would be predominantly utilised by the IT department. In addition, for Bank A and B, it is also seen to be most useful or consistently playing a critical role primarily in the pre-deployment stage, i.e. when the organisation is in the midst of establishing the AML/CFT IT solution. During this stage, the ability to establish appropriate technological infrastructure for AML/CFT purposes is frequently required by the IT department in order to facilitate the deployment of IT solutions that are in accordance to the expected regulatory deliverables.

The above situation can further be contrasted with the alternative stage (i.e. post-establishment). In this particular stage, it can be regarded that the ISI capability will
be less frequently needed by the IT department. Furthermore, at the point when modifications to the organisational IT infrastructure need to be carried out (i.e. such as due to the need to increase the technological capacity or further system fine-tuning), they can also be considered as ad-hoc activities. Therefore, the ISI capability can be seen as having a less significant role once the AML/CFT IT system has been successfully implemented.

b) IS Technical Skills (ISTS)

The ISTS capability from the perspective of regulatory compliance is defined as the: “ability of organisational IT staff to acquire, deploy and manage knowledge of IS technical skills that ensure effective IT deployment and operations that facilitate regulatory compliance.”

It is important to note that the ISTS capability in this context will only refer to the skills that are exclusively required to implement regulatory driven IT solutions. Therefore, this capability is foreseen to play an important role in ensuring smooth deployment of IT systems established for regulatory purposes. Nevertheless, arising from the flexibility of AML/CFT IT system implementation [see Section 8.2.3(a)], the ISTS capability can generally be regarded as not being typically required in deploying AML/CFT initiatives within the organisation.

It is interesting to note that views and opinions of research participants in Bank A and B have nonetheless suggested that there wasn’t any need to use the ISTS capability in facilitating AML/CFT compliance. Therefore, the capability to acquire, deploy and manage specific IT skills for AML/CFT deployment purposes could not be established or identified in these two organisations. One way of explaining this situation is from the viewpoint that the nature of ISTS capability that can typically be considered as generic and hence, not regulation specific. In other words, ISTS capability such as programming know-how is universal and not explicitly tailored to any particular IT solution. This is regardless of whether the system is to be developed for business purposes or intended to satisfy regulatory requirements imposed by the regulatory authority.
The above discussions can be further be seen in by the insights provided by the interviewees. In this regard, Bank A’s Head of Solution Delivery II had highlighted that there is “no specific IT skills” (036) uniquely required for the implementation of AML/CFT IT system in the organisation. Also, in a separate interview with the Head of Integrated Risk Management, the interviewee had also echoed the earlier notion by suggesting the generic nature of IT skills, which can be used “regardless of what the guidelines are” (037).

From another perspective, Bank B’s AVP from the IT department had suggested that the AML/CFT IT solution is merely a system that generates reporting and alerts. Therefore, specific IT skills can be regarded as not necessary:

“..... it’s just a simple thing. You set a limit... If you reached the limit, therefore create the alert, create the message. I mean, you can see the whole process as fundamentally that way ..... I view AML as very much a reporting [system].” (040)

The above view is further shared by a Compliance Manager, who had also mentioned that specific IT skills are not being needed to use the AML/CFT IT system:

“No, it’s very simple to navigate, in our system so we don’t really need to have specific skills ..... not so much of IT skills.” (028)

Similarly, the CIO from the same organisation was of a similar opinion regarding the absence of specific IT skills that is needed to ensure compliance with AML/CFT requirements. According to the interviewee, the IT skills are more generic, which also can be used for all systems in the organisation:

“..... basic technical knowledge, which is common. Let’s say I’m a developer, I know certain programming language, any platforms, so this is what I meant by the basics.” (029)

Interestingly, an interviewee from the regulatory authority also shares the same sentiment regarding the absence specific IT skills needed for compliance to AML/CFT requirements:
“Not specific on AML/CFT, no. It’s a normal IT skill. Because the rules are determined by the business units based on the experience. So now just to write a programme to detect... to cater for the detection rules, the called it.” (032)

Therefore, based upon the above discussions, it can be concluded that the ISTS capability foreseen to play an important role in ensuring smooth implementation of AML/CFT IT systems are not available in Bank A and B. Hence, in this regard, generic IT technical knowledge is deemed to be sufficient, as compared to the need to have specific technical skill for compliance purposes.

The above situation may partly be explained through the nature of the AML/CFT IT systems being deployed in Bank A and B. In this regard, as noted in Section 5.4.4, both organisations have been utilising off-the-shelf systems. This may influence the absence of any specific IT skills during the management and maintenance of these IT systems.

c) IS Development (ISD)

From the context of regulatory compliance, the ISD capability is defined as the: “ability to swiftly develop and implement IT solutions that are effectively addressing new or revised regulatory requirements.”

Similar to the discussion in Section 8.2.3(b), it is essential to note that the ISD capability will only be referring to the efforts required to develop and implement regulatory driven IT solutions. In addition, this capability is foreseen to play an important role in ensuring the implementation of IT system established for AML/CFT purposes is speedily developed within the organisation. However, since the development for the IT solution is not mandatory [see Section 8.2.3(a)], the ISD capability can generally be regarded as not being typically required in deploying AML/CFT initiatives within the organisation.

Nonetheless, it is essential to note that views and opinions of research participants have indeed suggested that no system development efforts were being utilised to establish the regulatory systems in Bank A and B. This is due to the understanding
that these systems are in effect, off-the-shelf in nature [see Sections 5.4.4(a) and (b)]. Rather, the utilisation of this specific capability can be regarded as more inclined towards performing data mapping and system configurations, as highlighted by Bank A’s Head of Analytics,:

“The work is more on the mapping the data from our host to the new system, configure the system... setting the threshold, risk profile... that kind of thing. It’s a ready system. You just need to configure it.” (001)

The above understanding can also be obtained from a separate interview with Bank A’s IT Department lead for the RSA2 system. In this regard, the interviewee had further highlighted the need to ensure that necessary information from multiple source systems be made compatible with the format specified by the vendor:

“..... I have so many source teams, they will be passing me a lot of files, from their respective systems, my team here what we do is, some of this files, we need to transform to put into the format that the vendor wants.” (004)

With regard to Bank B, although the effort on data extraction and cleansing process was not emphasised by the interviewees since the RSB1 system had already been implemented, it is sensible to assume that similar situation may have also occurred. This is due to the understanding obtained in Section 7.5.1, in which a separate information repository has been created for RSB1. In this regard, the repository is said to contain transactional information gathered from the EDW and several source systems. Therefore, the required cleansing process would be similarly required to ensure that a consistent and suitable format that matches the RSB1 system is achieved.

Moving on to the assessment on the speed of implementation, even though both organisations’ AML/CFT IT systems are off-the-shelf, there was little evidence to suggest that they were swiftly implemented as they had to go through the typical phases similar to the establishment of other IT systems in the organisation such as of data preparation process and testing. For example, for the case of Bank A, the Head
of AML/CFT and Compliance Strategy had mentioned an instance of slight delay occurring:

“Our focus now is to resolve the issue and bring it to UAT stage. Because rightfully, we are 2 weeks behind UAT” (034)

Therefore, the ISD capability can be regarded as being utilised by the IT department. In addition, it is also seen to be most useful during the pre-deployment stage of the AML/CFT initiatives. This is premised on the understanding that during this stage, the capability will be regularly needed by the IT department in an effort to facilitate the deployment of IT solutions that meet regulatory expectations.

The above situation can further be contrasted with the alternative stage (i.e. post-establishment). In this particular stage, it can be regarded that ISD capability will be playing a less significant role once the AML/CFT IT system has been completely and successfully implemented in the organisation, as further fine-tuning or system changes can be considered as an ad-hoc activities that are based on the merit of each case.

d) Cost-Effective IS Operations (CEISO)

The last capability under the inside-out categorisation of capabilities, i.e. CEISO capability can be defined as the: “ability to continually provide efficient and cost-effective IS operations that facilitate compliance to regulatory requirements.”

The CEISO capability in the context of AML/CFT IT systems can be regarded as the ability to ensure that possible ML/TF activities are efficiently monitored and detected by the IT solution, and all exceptions are flagged to be further reviewed by related members of staff in the organisation. Therefore, this capability is regarded to play an important role in the implementation of IT systems established for AML/CFT purposes. Nevertheless, since the deployment for the IT solution is not mandatory [see Section

---

47 Since Bank B had already implemented RSB1 for about three years [see Section 5.4.4(b)] at the point when the interviews were conducted, the progress of RSB1 system implementation was not emphasised.
Chapter 8: Analysis of Capabilities

8.2.3(a)], the CEISO capability can also generally be regarded as not being typically required in deploying AML/CFT initiatives within the organisation.

In the case of Bank A and B, as highlighted earlier, although IT systems for AML/CFT are not explicitly enforced, these organisations had nevertheless implemented their own regulatory IT solutions. This is arising from the understanding that manual monitoring are considered to be operationally unfeasible due to the large number of banking customers and high volume of daily transactions that these organisations are having. Therefore, it can be safely be interpreted that these organisations had implemented their IT solutions in order to be more efficient in the monitoring and detection of possible cases of ML/TF activities.

Hence, from the context of Bank A and Bank B, the CEISO capability can be regarded as having the tendency to be utilised by the IT department. This is because the general responsibility for ensuring efficient and effective organisational IT operations typically lies with this particular department. In addition, this capability is also seen to be most useful during the post-establishment stage of the AML/CFT initiatives. This is based on the comprehension that the organisation’s IT department will need to constantly ensure that the IT system for AML/CFT is running efficiently to ensure effective monitoring and detection.

The above situation can further be contrasted with the alternative stage (i.e. pre-deployment). In this particular stage, it can be regarded that CEISO capability would be less needed as the effort to mitigate the risk of ML/TF has yet to be established as part of the organisation’s IT solution.

8.2.4. Spanning Capabilities

The third category of capabilities are known as spanning capabilities and are used to integrate the earlier two categories of capabilities i.e. outside-in and inside-out. The two capabilities that have been classified under this type of capability are IS-Business Partnerships (ISBP); and IS Planning and Change Management (ISPCM). Their roles in
influencing and aiding the attainment of compliance benefits through the activities of complying with the requirements on AML/CFT are explained in the following sections.

a) IS-Business Partnerships (ISBP)

The ISBP capability from the perspective of regulatory compliance is defined as the: "ability to integrate and align IS function with other functional areas within the organisation in order to assist in the compliance efforts."

The IS function in this context can be regarded as the particular division within the IT department that is accountable to facilitate the implementation of regulatory IT solutions. Therefore, the ISBP capability from the context of AML/CFT can be viewed as the ability for this division to obtain the necessary cooperation and information from other related departments in order to establish the regulatory IT system. Hence, this capability can also be regarded as typically required for AML/CFT IT deployment as it ensures smooth implementation of the organisation’s overall AML/CFT initiatives.

It is important to note that, as can be seen in the earlier Figure 8-3, the two internal key stakeholders for the IT department (i.e. within the organisational boundary, as depicted by the circular dotted line) is regarded as the various related business departments in the organisation, as well as, the Compliance department.

From the perspective of the relationship with the first key stakeholder (the various business departments), the utilisation of ISBP capability can be regarded as valuable and essential. This situation arises from the earlier appreciation that related information need to be acquired from various business IT systems to be an important input to the AML/CFT IT system. As previously highlighted in an earlier discussion [see Section 8.2.3(c)], Bank B’s transactional information were gathered from the EDW and several source systems for the purpose of its RSB1 system. Furthermore, a similar
situation has also occurred in Bank A, where transactional information was also made available in an information repository established for the RSA2 system.\(^{48}\)

Therefore, arising from the above, cooperation and commitment from the respective systems or repository owners to provide these informational inputs is paramount in order to ensure that the needed information is successfully integrated within the AML/CFT IT system. In this regard, the IT department will accordingly need to efficiently coordinate and interact with multiple teams, in order to achieve the needed collaboration with business users from related products, together with their respective IT support teams and vendors.

In relation to the views and opinions of research participants, instances where this particular capability is being utilised can be appreciated by the statements made by the interviewees. In this regard, Bank A’s IT Department lead for the RSA2 system had highlighted the need to intensely liaise and interact with various parties within the effort to establish the RSA2 system:

“[Previous interactions were] not that extensive ..... In this [RSA2 system] case, the business users have already indicated that they want to track all high-risk products. ..... Prior to RSA2, yes, we have been liaising with any of these IT teams but on a smaller scale. ..... But for this new AML project, I’m liaising with five, six teams, additional teams.” (004)

Moving on to the perspective of the IT department’s relationship with the second key stakeholder, i.e. the Compliance department, the utilisation of ISBP capability can also be regarded as critical and important. The significance of this capability can be seen through the needed collaboration between IT and the Compliance departments during the course of implementing the AML/CFT IT system. In this regard, it is commonly expected that the IT departments in both organisations to constantly and closely liaise with the owner of their AML/CFT IT systems, i.e. the Compliance department, during the development of the IT solution.

\(^{48}\) For Bank B, the source systems are; conventional banking; Islamic banking; auto finance; trade finance; credit card; and trading room system. Meanwhile, for Bank A, besides the GDW, other source systems are; current; savings; loans; credit cards; fixed deposits; auto finance; insurance; and stock broking system [see Section 7.5.1].
Therefore, the capability for IT to collaborate with the Compliance department can be equally considered as vital and critical in order to ensure that the regulatory system being developed accomplishes the specifications outlined by the system owner, as well as satisfies the expectations of the regulatory authority. For instance, Bank A’s IT Department lead for the RSA2 system had further elaborated about the importance of collaborating with the business users:

“Oh yes, definitely because we have a lot of interactions not only with the IT teams, but also we have to interact with the business users. .... For us to do the transformation [i.e. data cleansing], we don’t just simply transform based on our knowledge, we get the business users to concur or to decide what’s the mapping that we need to do.” (004)

Therefore, as can be seen from the above discussions, the ISBP capability seemed to be utilised by the IT department. In addition, it is regarded to have played a significant role during the pre-deployment stage of the AML/CFT IT solution. During this stage, the capability is regularly needed by the IT department to liaise with the related departments in the effort to facilitate the deployment of IT solutions that meet regulatory expectations.

The above situation can further be contrasted with the alternative stage (i.e. post-establishment). In this particular stage, it can be regarded that the ISBP capability will be playing less significant role once the AML/CFT IT system has been completely and successfully implemented in the organisation.

b) IS Planning and Change Management (ISPCM)

The ISPCM capability from the context of this research is defined as the: “ability to anticipate future changes and expansions arising from new or amended regulatory demands, by planning, managing and using appropriate technology.”

---

49 Throughout the interviews, the Compliance department is also often considered as a business user from the viewpoint of the IT department. This situation can be explained from the understanding that any system users that do not originate from the IT department are typically considered as non-IT users, and therefore, they are often being commonly grouped as the general business users of the organisation.
As has been acknowledged in Section 2.4.2, regulatory requirements are hardly ever revoked. Importantly, new and greater requirements seemed to continue to be implemented (Elliehausen, 1998). Therefore, arising from this general understanding, it is essential for organisations to employ proper planning and management to anticipate revisions to their regulatory IT system, especially arising from possible new developments in the regulatory environment. Hence, this capability is typically required in order to ensure that a regulatory compliance system be kept relevant and up to date.

However, from the context of AML/CFT IT implementation, views and opinions of research participants seemed to suggest that new or revised AML/CFT regulatory requirements are not anticipated to be issued by the regulatory authority. Hence, there is little evidence to suggest that the ISPCM capability has been utilised to plan and manage possible revisions in requirements that may impact the organisation’s AML/CFT IT system. For example, during an interview with Bank A’s Head of Analytics, the interviewee had suggested that new requirements on AML/CFT are highly unlikely:

“I think nothing much in that area [i.e. regarding the possibly of new requirements]. If there is a new requirement, I think that is more on the enforcement of investigation part.” (001)

The above opinion regarding the improbability of new AML/CFT requirements being enforced was also echoed by Bank B’s Vice President for Consumer Bank Risk Monitoring. The interviewee had instead forecasted about the likelihood of more information on sanctions to be issued:

“I see more sanctions ..... new sanctions on Iran. The new resolution 1929, and the new OFAC sanctions on Iran. So these are the things that we need to comply also.” (006)

It is worth reiterating at this juncture about the need to ensure the names of known terrorists and money launderers, as well as the list countries under surveillance to be continuously kept updated in the organisation [see also Sections 6.3.5 and 6.3.6]. While the above requirements can be treated as another form of system changes that may need to be carried out whenever there are any new updates, the effort to
achieve this objective can safely be regarded as trivial. This situation may partly be attributed to the type of AML/CFT IT system being used in Bank A and B, which are off-the-shelf in nature. Hence, any modifications needed to suit previously mentioned updates will typically require mere parameter changes.

Therefore, arising from the above discussions, it can be concluded that the utilisation of the ISPCM capability is rare in Bank A and B. This is primarily due to the understanding that new or revised AML/CFT regulatory requirements are not anticipated to be issued by the regulatory authority.

8.2.5. Additional Capabilities for Compliance Benefits

Overall, there are three additional capabilities that have been detected from the interview data, which are not regarded to be part of the list of capabilities suggested in Section 3.4.2. These additional capabilities are: Compliance-Business Partnerships (CBP); Business Knowledge (BK); and Analytical and Investigational Skills (AIS). It is important to note that these additional capabilities should be considered as only specifically associated with the effort to implement AML/CFT initiatives in the organisation, and further aid in achieving compliance benefits. These additional capabilities can also be seen as having more inclination to be viewed as organisational capabilities, rather than technical capabilities, necessary to implement AML/CFT requirements.

The following sections will discuss each additional capability in detail. It is worth noting at this point that the discussion on these capabilities will not be presented according the classifications of IS capabilities utilised in the earlier section (i.e. outside-in; inside-out; and spanning). This specific approach is taken with the aim to distinguish these capabilities from the ones suggested in Chapter 3.

a) **Compliance-Business Partnerships (CBP)**

The CBP capability from the perspective of AML/CFT implementation can be *defined* as the: "ability of the compliance function to interact and obtain the necessary
cooperation and information from other functional areas within the organisation, with the objective to assist in the compliance efforts.”

The ability of Compliance department to initiate collaborations with the business departments need to be explicitly highlighted. This arises from the understanding that the implementation of organisational AML/CFT initiatives are typically led and overseen by the Compliance department [see also Section 5.3.1(b)]. This capability can therefore be regarded to be typically required for establishing and deploying regulatory IT systems, as it ensures the necessary cooperation and information are obtained from other related departments.

In relation to the views and opinions of research participants, instances where this particular capability is being utilised can be appreciated through the insights obtained from the interviewees. For example, it has been discovered that Bank A’s Compliance department had interacted with, and sought the cooperation from, relevant business departments. As related by the Head of Analytics, this was done with the aim of obtaining the necessary information for establishing customer risk profiling information in its AML/CFT IT system:

“During the earlier part of implementation, initial phase, we called all the interested parties. ..... people from host, data warehouse, even CRM also, because initially what we were planning to do was actually to take the information from them for AML profiling.” (017)

It is important to also note that, as suggested by the same interviewee, the interactions between Compliance department and relevant business departments had also continued beyond the initial discussions held during the early stages of the AML/CFT IT implementation:

---

50 The interactions between the compliance and IT departments are not covered by this capability, but instead fall under the ISBP capability [see Section 8.2.4(a)].

51 The last sentence in this particular interview statement was purposely removed as it was pointing towards to the notion of supplementary benefits. The full interview statement will again be presented in Section 8.3.5(a), which will elaborate on the capabilities that are seen to have influenced the creation of supplementary benefits in Bank A.
“Even as at now, during the development phase, we have been in touch with a lot of parties, like GCIF, CRM, and the National Sales Department.” (017)

It needs to be clarified that a similar nature of working relationships between Compliance and the business departments was not detected in Bank B. Nevertheless, it is sensible to assume that organisations will need to have some form of interactions with the business departments. This is can be credited to the situation where the information required for AML/CFT effort, is in effect, residing in various source systems owned by the business.

The general sentiment on the importance of interacting with the business departments was also detected during an interview with the Head of Compliance and Corporate Secretary from a foreign banking institution. In this regard, the interviewee had highlighted the need to “sit down” and interact with the business:

“So to implement any guidelines for that matter, we will always have to sit down with the business, to understand for example we’ll ask them what kind of customers do you have, what’s your general threshold of your customers, when do you deemed your customer is a high-risk.” (013)

Even though this capability has been regarded as typically required for establishing AML/CFT initiatives, it is also seen to be useful when the organisation’s AML/CFT initiatives have been fully deployed and operational. In this regard, the CBP capability that enables the Compliance department to interact and collaborate will also be valuable in the form of assisting and guiding the business departments during the effort to ensure compliance to regulatory requirements.

In both Bank A and B, their Compliance departments have more or less applied the same approach in relation to the intention to achieve effective implementation of AML/CFT effort in their organisations. As has been seen in Chapter 7, this is done through interacting and providing business departments with guidance on, among others; complying with regulation; interpretation of requirements; obtaining “buy-in” in terms of educating; and obtaining commitment to compliance matters [see Sections 7.6.1(b) and (c)].
Therefore, arising from the above discussions, the CBP capability will primarily be utilised by the Compliance department. In addition, this capability is seemed to exhibit equal qualities to be regarded as playing a significant role in both stages of the AML/CFT implementation (i.e. pre-deployment and post-establishment). In the pre-deployment stage, the capability will be mainly needed to solicit the required information, as they are mainly residing in the various source systems owned by business departments. Meanwhile, in the post-establishment stage, the capability will be useful to assist and guide business departments to ensure compliance to AML/CFT regulatory requirements.

b) Business Knowledge (BK)

The BK capability from the perspective of AML/CFT implementation can be defined as the: “ability to comprehend the general banking operations, as well as understanding the products and services of the organisation.”

The criticality of BK capability can be explained from the differing perspectives of the two departments that are seen to be actively involved in the AML/CFT IT system implementation process (i.e. the Compliance department, and the IT department). From the Compliance department’s viewpoint, having adequate knowledge on banking operations, as well as understanding organisation’s products and services are indeed critical. A sufficient knowledge on these areas will allow the AML/CFT control measures to be effectively deployed, as well as ensuring that they are practical and implementable. It will essentially be challenging for operational departments to meet AML/CFT requirements if policies and procedures established by Compliance department only look good on paper, but are lacking in practical and effective implementations. Hence, it is vital for Compliance department to exhibit this capability during the implementation of AML/CFT efforts in the organisation.

On the other hand, from the standpoint of the IT department, by having BK capability, the department will be able to view the system from the users’ perspectives, and therefore will be better equipped to deploy a system that will be aligned with the intended outcomes and closely meeting users’ expectations. Therefore, as a whole,
this capability can be considered to be typically required as it ensures effective implementation of the AML/CFT IT system within the organisation.

The importance of having BK capability can be detected in the views and opinions of research participants. One of the best examples would be from the insights provided by the Head of Compliance from a local banking institution. According to this interviewee, by having sufficient experience and product knowledge, the staff from Compliance department will not be “so academic” as they understand the business and appreciate the associated risks. The department was also not seen to be encountering any significant resistance during its AML/CFT implementation, as they were basically “speaking the same language”:

“I’ve gone for people which have got ground and product knowledge because of two purposes. One, they understand the business. Second, because they came from business, and they got involved in risk, that means they appreciate the need for risk. So they won’t be so academic.” (021)

“I guess that’s another benefit as to why I don’t get such resistance from the business, because if they deal with me or any of the managers, you’re basically speaking the same language.” (021)

It is acknowledged that not all organisations were experiencing the privilege of having their Compliance staff with extensive business working experience. However, the importance of having this type of knowledge will also certainly be a significant advantage during the implementation of AML/CFT initiatives. As related by the Head of Group Compliance from another local banking institution, the preference of employing new Compliance staff would primarily be based on their understanding of banking business, as well as ability to appreciate banking transactions:

“The preference is for people who have worked in banks before, so that they will understand banking transactions. Because they will be monitoring, banking transactions. So if you don’t understand banking transactions, it will be a bit difficult.” (020)

Meanwhile, insights from the interviewees specifically from the standpoint of the IT department can likewise be noted. For example, Bank A’s Head of Integrated Risk
Management had suggested that it is a common expectation for the IT department to be having a thorough understanding on the business flow:

“There’s always this expectation that we understand the business flow thoroughly.” (037)

Furthermore, a CIO from a foreign banking institution had highlighted the need for staff of IT department to possess business knowledge. This is required as to increase their understanding from the users’ perspective:

“..... business and operational knowledge ..... we IT people need to know how it works, who uses it. If the customer involved, how do they use it, what do they need.” (029)

Therefore, arising from the above discussions, the BK capability seemed to have the tendency to be utilised by both the Compliance and IT departments. Similarly, it is regarded to be most useful or consistently playing a critical role during the pre-deployment stage, i.e. when the organisation is in the midst of establishing the AML/CFT IT solution. In this stage, the capability will be frequently needed by both departments in order to ensure that control measures implemented are effective, practical and feasible to the organisation.

It is also worth highlighting at this juncture that during the post-establishment stage, the importance of BK capability in the organisational implementation of AML/CFT initiatives should not entirely be ignored. As seen in one of the interview statements above, it is sensible to conceive that this capability would also be critically required by the Compliance department in determining the accuracy of the alerts being generated by the AML/CFT IT system. In this regard, the Compliance department’s staff responsible to review the alerted transactions will require general comprehension on banking operations, as well as understanding the products and services of the organisation. These various aspects of business knowledge would be highly critical for the staff to determine whether the alerted transactions are confirmed suspicious or otherwise.
c) **Analytical and Investigational Skills (AIS)**

The AIS capability in relation to this research can be defined as the: “ability to conduct comprehensive and thorough analysis, as well as to effectively scrutinise and inquisitively examine ML/TF suspicious cases that have been flagged off by the detection mechanisms.”

This capability is critically required for AML/CFT implementation as it is highly useful during the CDD process in determining the accuracy of alerts that have been triggered. This capability can be used to perform a comprehensive analysis without hurriedly forming a judgement. Furthermore, via a thorough initial investigation and good STR documentation, they can provide good leads for the regulatory authority to pursue the matter further. Therefore, this capability is extremely important in the organisation’s efforts to mitigate the risk of ML/TF, and can thus be regarded as typically required in an AML/CFT implementation.

The significance of having the AIS capability can be detected in the views and opinions of research participants. For instance, a Compliance Manager had specifically highlighted the need to have staff with inquisitive skills:

“I only need people who have curious minds, when you do this type of job...”

(028)

The above view is also shared by a Head of Operations Risk and Compliance. This interviewee had explicitly mentioned the need for relevant staff to perform adequate analysis, without hastily forming an opinion or passing a judgement:

“..... they need to be very sharp in analysing situations. Sometimes you just [tend to] jump into conclusion on a lot of things.” (014)

On a slightly different perspective, but nevertheless contributing to the discussions, Bank A’s Head of Group Compliance had interestingly mentioned about the superiority of the organisation’s STRs. Arising from “systematic and dynamic” initial investigations conducted, comprehensive STRs were able to be developed and submitted to the regulatory authority. This situation had further provided excellent
leads for the regulatory authority to pursue with further investigations or prosecutions, if deemed necessary:

“I mean the method of investigation is more systematic and dynamic. It has assisted the bank to develop good STRs. [The STRs are] also for the regulator to actually view and review the investigation, and as a good lead to prosecute or leading to the real investigation by the law enforcement agencies.” (008)

The same interviewee from Bank A had also provided useful insights into the distinctive fact-finding nature of the organisation’s staff responsible. In this regard, the interviewee had mentioned about the staff concern had gone undercover in order to produce a good report for the regulatory authority:

“….. they have also come to the stage whereby they had gone undercover. Meaning to say, they went into the operations itself, they went to the site ….. get the right information, and had resulted a good report and for the authorities to investigate and proceed with their whatever actions that they want to take ….. And this is probably because my staff that did the investigations actually have an investigative type of mind.” (008)

Therefore, arising from the above discussions, the AIS capability seemed to have the tendency to be utilised by the Compliance department. In addition, it is regarded to be most useful or consistently playing a significant role during the post-establishment stage, i.e. upon the complete and successful implementation of AML/CFT initiatives within the organisation. This is based on the understanding that the Compliance department will need to constantly analyse and investigate alerted transactions during the effort to understand the modus operandi and further mitigate the risk of ML/TF activities.

The above situation can further be contrasted with the alternative stage (i.e. pre-deployment). In this particular stage, it can be regarded that this capability would be less needed as the effort has yet to be established as part of the organisational practices. Therefore, the situation has yet to reach the stage where the capability would be critically and continuously required.
8.2.6. Summary and Conclusion

In summary, the analysis has provided empirical evidence to suggest that not all the capabilities identified by Wade and Hulland (2004) are equally influential in facilitating the realisation of compliance benefits from AML/CFT IT implementations. Importantly, it has also suggested that the need of additional capabilities in achieving a similar objective. In addition, while some capabilities were seemed to be more useful in a particular stage of the implementation, there are other instances where capabilities are regarded to be highly required in both stages. A similar principle also applies to the department that was seen to have the tendency to utilise these capabilities. In this regard, both Compliance and IT departments may need to use some of these capabilities in ensuring compliance, and thus achieving compliance benefits. The following Figure 8-4 graphically summarises the discussion by presenting the nature of relationships between the identified departments, stages, and capabilities in achieving compliance benefits to the organisation:

![Figure 8-4: Relationships - Department, Stage, Capability & Compliance Benefits](image-url)

ERM: External Relationship Management
MR: Market Responsiveness
ISI: IS Infrastructure
ISTS: IS Technical Skills
ISD: IS Development
CEISO: Cost-Effective IS Operations
ISBP: IS-Business Partnerships
ISPCM: IS Planning and Change Management
CBP: Compliance-Business Partnerships
BK: Business Knowledge
AIS: Analytical and Investigation Skills
8.3. CAPABILITIES FOR SUPPLEMENTARY BENEFITS

8.3.1. Overview and Specific Approach

With reference to the earlier discussion on capabilities for compliance benefits in Section 8.2, it was found that only a few of these capabilities were regarded as having facilitated the realisation of supplementary benefits. For this reason, the presentation on the analysis of capabilities for supplementary benefits has also adhered to the following approach:

i). The extended analysis and discussions will *only* be confined to the set of capabilities that were deemed to have exclusively facilitated this type of benefit. In this regard, these identified capabilities can also be regarded as the ones that have been utilised beyond the basic activities of AML/CFT implementation within the organisation;

ii). In addition, the analysis will *only* be done from the perspectives of Bank A. Briefly summarising the understanding gained from Chapter 7, the decision to focus on this organisation arises from the understanding that Bank A has been *and* is likely to continue experiencing supplementary benefits [see also Sections 7.5.1 and 7.6.1]. This is in contrast to the situation affecting Bank B, which has yet to experience all the supplementary benefits highlighted in Chapter 7. Therefore, it can be concluded that the usage of the capabilities that have influenced the achievement of supplementary benefits *are not* commonly experienced by all organisations;

iii). The successful identification of these capabilities has also set the scene for further assessment of business advantages. In this regard, the study will attempt to comprehend how the utilisation of these capabilities, in facilitating supplementary benefits, is likely to influence the competitive positioning of Bank A. Capabilities utilised by Bank A to achieve supplementary benefits can be regarded as a good candidate to assess business advantages. As revealed by the literature (e.g. Doherty and Terry, 2009), the accomplishment and sustainability of organisation’s competitive positioning is highly related to its ability to deploy an appropriate selection of IS capabilities. Hence, the research will be adopting a similar
Chapter 8: Analysis of Capabilities

perspective in an effort to determine any instances of business advantages that may emerge in Bank A;

iv). The assessment of business advantages for Bank A will be premised upon the attributes initially described in Chapter 3 (i.e. value; rarity; and appropriability). The assessment will also aim to denote the possibility of the organisation achieving improved competitive positioning (ICP), and therefore, it will not be indicating that a clear competitive advantage has been achieved [see Section 3.4.3].

It is essential to appreciate further that the definitions for value and appropriability are based upon those suggested in Chapter 3, and be used in the assessment for the capabilities identified in this section. Nevertheless, modifications to the definition of the rarity attribute is needed in order to allow for a clearer and more suitable description, as well as enable for it to be accurately utilised in the research. This is arising from the understanding that since the identified capabilities are considered to be widely accessible as they are commonly utilised to firstly establish and deploy AML/CFT efforts in the organisation, they could not necessarily be considered as rare. In this regard, the capability itself is not to be regarded as exceptional, even though it has been used to achieve supplementary benefits. Therefore, to address this unique situation, definition for rarity attribute will need to instead refer to the unusual usage of these capabilities. Hence, in specific relation to this research, the rarity attribute will be referring to the: “unusual and exceptional usage of the capability to achieve supplementary benefits, which is not widely and similarly utilised by other organisations in a simultaneous manner.”

v). The assessment of business advantages will not be considering capabilities that are regarded as facilitating compliance benefits. It was previously envisaged that compliance benefits could also possibly influence the organisation’s competitive

---

52 The research will not be extending the assessment on capabilities to evaluate their potential to attain sustained competitive advantage (SCA). This decision arose from the understanding that one of the conditions for the assessment of attributes for SCA (i.e. low imitability: the ability to protect the advantage from imitation) could not be met since the capabilities themselves are generically used to meet regulatory compliance and therefore, to attain compliance benefits for the organisation.
positioning through *uniquely* deploying effective compliance activities, and reducing compliance cost [see Section 3.3.4]. However, arising from the outcome of the preliminary analysis for RO1a [see Section 5.3.1(a)], there is no evidence to support the earlier assumption. Therefore, assessing compliance benefits from the perspective of competitive positioning is no longer a sensible approach;

vi). Due to the appealing possibilities of these capabilities to influence the organisation’s competitive positioning, this analysis will also be attempting to highlight the nature of relationship between the identified capabilities and the supplementary benefits that they are most likely to be influencing. In this regard, the research attempts to ascertain from the perspective of how the realisation of supplementary benefits is being directly or indirectly facilitated by these identified capabilities. This standpoint takes into consideration that the identified capabilities are not intended to be explicitly utilised to generate supplementary benefits at the onset. Rather, they can be regarded as the common capabilities for organisation’s compliance activities, but have been acknowledged to be unusually used to facilitate and aid the generation of supplementary benefits.

The rest of the presentation in this section will continue to discuss on each capability, explaining its role in facilitating the attainment of supplementary benefits. In addition, the discussion will also utilise the same approach adopted in Section 8.2, by first presenting the identified capabilities according to the classification suggested by Wade and Hulland (2004). This will then be followed by a similar presentation on the associated additional capabilities. In addition, for each capability, further assessments will also be done from the perspective of competitive positioning. This will be conducted before the whole section is ended with a presentation of the summary and conclusion.

Importantly, the presentation for *each capability* under this section will also tend to utilise a similar sequence of presentation as mentioned in Section 8.2. In this regard, the presentation will start by presenting the rationale on its significance. Where available, relevant interview quotes expressing the views and opinions of the research participants are also presented in order to provide further explanation to the discussion. Importantly, the presentation will also capitalise on the extensive
discussion and understanding obtained from the previous analysis chapters, as well as the earlier discussion on capabilities for compliance benefits. Finally, a brief discussion on the *departments*, as well as the relevant *stages* relating to each capability will also be done at the end of each section.

In addition to the above, a structured presentation via an *evaluation table* will also be made available at the end of the discussion for each capability. The evaluation table in this regard, aims to systematically assess the role of the capability in possibly influencing the competitive positioning of Bank A, by using the attributes that have been discussed earlier in Section 8.3.1(iv).

### 8.3.2. Outside-in Capabilities

For the first category, *only one* out of the two capabilities has been considered to be influencing the attainment of supplementary benefits through AML/CFT IT implementation. The identified capability in this regard is the ERM capability, and the rationale for this situation to occur will be further elaborated in the section that follows.

a) **External Relationship Management (ERM)**

From the perspective of Bank A, there is little evidence to suggest that the capability to manage the relationship with two of the key external stakeholders has played a role in accomplishing supplementary benefits.\(^{53}\) In this regard, the interactions with the regulatory authority, as well as the hardware vendor have not been considered to have gone beyond the needed basic assistance, cooperation and information to effectively implement AML/CFT initiatives in Bank A.

On the other hand, interactions with another key external stakeholder, i.e. the software vendor, have been considered as positively influencing the attainment of supplementary benefits in Bank A. These interactions have been seen as providing the

---

\(^{53}\) As mentioned in Section 8.2.2(a), the three key external stakeholders for AML/CFT deployment are the regulatory authority, as well as the AML/CFT software and hardware vendors.
organisation with the opportunity to leverage the vendor’s expertise and previous experience, as well as being made aware of system functionalities that can be used beyond AML/CFT compliance.

The views and opinions of research participants will be able to provide deeper insights into the above statement. In this regard, the Head of Analytics had acknowledged the contribution of the software vendor, when asked about the how the business benefits from the implementation of AML/CFT IT system was initially discovered:

“I would say mostly come from the vendor itself. When they presented the system, they did share the capabilities of the system and how other users are using it. Things like data mining for, let’s say for credit card usage or remittances for high net worth customer ..... The vendor shared with us how other banks are using the system to capitalise on marketing or other areas.”

(017)

It is essential to note at this juncture that the sharing of expertise and experience by the software vendor does not necessarily guarantee that the Compliance department will derive business benefits from their regulatory related efforts. A contrasting viewpoint, to Bank A’s, was detected during an interview with the Head of Compliance from a local banking institution. In this regard, the interviewee had specifically stressed that any software vendors suggesting possible business value that can be obtained through AML/CFT IT system’s implementation will definitely be declined and not included in the vendor selection. The interviewee had strongly advocated that the AML/CFT IT system should only be intended to solely satisfy regulatory requirements, and nothing else:

“..... the only reason that we are looking at all of these [potential IT solutions] is because it’s for regulatory requirements. And the guys who are really into the business will know that they are going to find a person like me who are

---

54 Although it has been mentioned in Section 8.3.1(i) that the discussion on capabilities for supplementary benefits will only be done from the perspective of Bank A, the viewpoint revealed by this particular interviewee need to be critically highlighted. This is done to showcase the existence of an extreme contrasting approach, as opposed to the one adopted by Bank A.
going to kick them out if they come here and tell me they’re here to market [something else].” (021)

“That is my priority. So I don’t want to look at vendors who looks at it as by the by. That’s means it’s like AML [functionalities] is one of the things that they sell.” (021)

Having viewed the above contrasting standpoints, it can therefore be regarded that Bank A’s Compliance department has taken the option to appreciate the suggestions made by the software vendor. Therefore, interactions with the software vendor can be considered to be one of the underlying factors that had introduced the idea of attaining business benefits to Bank A’s Compliance department.

Moving the discussion to the specific supplementary benefits that have been regarded to be influenced by the ERM capability, a particular type of benefit is seen to have been realised. In this regard, the organisation’s ability to leverage the functionalities of fraud monitoring and detection were influenced by Bank A’s preparedness to utilise this capability. In other words, the ability to leverage the vendor’s expertise, experience, knowledge on system functionalities, has provided the foundation for Bank A to appreciate, and subsequently use the extra functionalities for fraud, within the AML/CFT IT system. By doing so, the organisation will be able to effectively mitigate the associated financial losses arising from possible fraudulent activities occurring within the organisation. Furthermore, as mentioned in Section 7.4.1, it is worth reiterating that since fraud functionalities are not part and parcel of the requirements to deploy AML/CFT measures, the usage of these functionalities has indeed brought benefit to the organisation.

Therefore, arising from the above discussions, the ERM capability can be regarded as having the tendency to be utilised by Bank A’s Compliance and IT departments during the pre-deployment stage, in the attempt to use the extra functionalities for fraud monitoring and detection within the AML/CFT IT system. Hence, through the usage of this particular capability, related parties within a business department will then be able to effectively monitor and detect fraud activities that may be occurring within the organisation, during the post-establishment of the regulatory system.
The following evaluation table provides a structured understanding on how the usage of ERM capability in influencing the occurrence of supplementary benefits, will further likely lead to an improved competitive positioning for Bank A. In this regard, the assessment will be done according to the three attributes that have been discussed in the preceding Section 8.3.1(iv). As shown in the assessment provided below, as a whole, the ERM capability does not seemed provide any form of business advantages to Bank A, unfortunately. This situation can be attributed to its nature of not seemed to possess the attributes of rarity:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Definition</th>
<th>Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>Allow the implementation of strategies that enhance efficiency and effectiveness</td>
<td>Yes. The ERM capability has enhanced the efficiency and effectiveness of the implementation of AML/CFT IT system. This is achieved through the ability to leverage software vendor’s expertise, experience, and knowledge on the system’s extra functionalities, particularly regarding fraud monitoring and detection.</td>
</tr>
<tr>
<td>Rarity</td>
<td>Allow exceptional usage of the capability that are not widely and similarly utilised by a huge number of organisations at the same time</td>
<td>No. The ERM capability has not enabled exceptional usage of fraud functionalities in the AML/CFT IT system. This is due to the understanding that the vendor is in effect, sharing what has been done by other banks. In addition, utilising fraud functionalities in the regulatory system need to be considered as a logical action to be made by the organisation [see also Section 7.4.1].</td>
</tr>
<tr>
<td>Appropriability</td>
<td>Ability to obtain returns accruing from the advantage</td>
<td>Yes. Through the usage of the ERM capability in assisting the establishment of fraud monitoring and detection capabilities, the organisation was able to obtain returns from the efforts made. This is in the form of being able to protect the organisation’s profits from possible monetary losses due to fraud committed by customer, as well as the bank’s staff.</td>
</tr>
</tbody>
</table>

8.3.3. Inside-out Capabilities

From the four capabilities in this category, i.e. ISI; ISTS; ISD; and CEISO, only two capabilities (i.e. ISI and CEISO) have been seen to be influencing the accomplishment of supplementary benefits through AML/CFT initiatives in Bank A. The following
sections will discuss in further detail regarding their influence in achieving supplementary benefits for Bank A.

a) IS Infrastructure (ISI)

As mentioned in Section 8.2.3(a), it has been regarded that an IT solution would be highly critical for Bank A, attributing to its nature of operations. Equally, the ISI capability that facilitates the establishment of this IT solution would also be similarly critical for the organisation. Arising from this situation, and due to the importance of Bank A’s AML/CFT IT solution, this IT system has also been regarded as one of the main driving factors that facilitate and influence the achievement of various types of supplementary benefits in Bank A.

One of the most important supplementary benefits identified in Chapter 7 that are being considered to be highly influenced by this capability is the opportunity to leverage the institution’s regulatory IT repository and directly benefit banking business [see Section 7.5.1]. In this regard, the repository of customer transactional information built for AML/CFT purposes has indeed been leveraged by a business department for their daily operations.

Briefly reiterating the important points from Section 7.5.1, customer transactional information originally sourced from multiple systems in Bank A, was subsequently cleansed and stored in the central repository. Subsequently, the transactional information this repository had become one of the most important and significant informational inputs for a system owned by the CRM department. From the perspective of this department, the transactional information from the regulatory IT repository has been regarded as a “single source of truth” as matters pertaining to missing, incomplete data and inconsistent formatting have been adequately addressed. In addition, as customer transactional information was not available in a single repository prior to the establishment of the central repository, it can therefore be regarded that the capability to establish appropriate IT infrastructure for regulatory purposes had indeed directly facilitated supplementary benefits for Bank A.
Besides the significance of ISI capability in establishing the necessary IT infrastructure and subsequently being leveraged by the CRM department to benefit business, it also essential to reflect on other instances of supplementary benefits that have been identified in Chapter 7. In this regard, it needs to be noted that all these supplementary benefits are, in effect, being made possible, as well as being made more effective arising from the implementation of the regulatory IT system. Hence, with that in mind, the supplementary benefits outlined in the preceding chapter can also be regarded as being influenced by the usage of ISI capability, to some extent.

Therefore, the ISI capability can be regarded as having a tendency to be utilised by the IT department during the pre-deployment stage, in the attempt to establish appropriate IT infrastructure for AML/CFT. Hence, arising from the usage of ISI capability to establish a regulatory IT infrastructure, a business department has been given the opportunity to leverage cleansed transactional information from an IT repository to directly benefit banking business. Nevertheless, this situation will only be achieved during the post-establishment stage, i.e. when the IT infrastructure has been fully complete and successfully implemented.

The following evaluation table provides a structured understanding on how the usage of ISI capability in influencing the occurrence of supplementary benefits, will likely lead to an improved competitive positioning for Bank A. Similarly, the assessment will also be done according to the three attributes that have been discussed in the preceding Section 8.3.1(iv). As shown in the assessment provided below, as a whole, the ISI capability does seemed to provide some form of business advantages to Bank A, due to its nature of possessing all the attributes being assessed:
Table 8-2: Business Advantages of ISI Capability

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Definition</th>
<th>Assessment</th>
</tr>
</thead>
</table>
| **Value** | Allow the implementation of strategies that enhance efficiency and effectiveness | • Yes. The ISI capability has provided value to Bank A in the form of establishing the dependency of the CRM department to a system exclusively established for regulatory purposes. This has therefore enhances the operational efficiency and effectiveness of the CRM1 system, through the act of leveraging the regulatory IT repository.  
• To a lesser extent, the ISI capability is also regarded to be able to efficiently facilitate the utilisation other type of supplementary benefits that has been identified by the research. |
| **Rarity** | Allow exceptional usage of the capability that are not widely and similarly utilised by a huge number of organisations at the same time | • Yes. In specific relation to the situation affecting the CRM department, the ISI capability has exceptionally facilitated a business department’s dependency on an information repository established for regulatory purposes, and subsequently been used to directly benefit banking business. |
| **Appropriability** | Ability to obtain returns accruing from the advantage | • Yes. The ISI capability has provided returns in terms of effective and efficient implementation of the CRM1 system, by accessing the regulatory IT repository of transactional information.  
• Additional returns are also in the form of other supplementary benefits being made possible, as well as being made more effective arising from the implementation of the regulatory IT system. |

b) **Cost-Effective IS Operations (CEISO)**

From the context of AML/CFT, cost-effective IS operations is achieved when all possible ML/TF activities are efficiently monitored and detected by the regulatory IT solution, and all exceptions are flagged to be further examined to determine its authenticity and legitimacy.

In the context of supplementary benefits, the need to ensure AML/CFT implementation is efficient and cost-effective has also provided the opportunity for Bank A to enhance their overall IT operations efficiencies. In somewhat similar perspective from the discussion for the ISI capability in the previous section, cleansed transactional data acquired from the regulatory IT repository have provided the CRM department with a speedier turnaround time in obtaining the needed information. As mentioned by the Head of CRM, this has been done as it would be inefficient for the
CRM1 system to obtain the required information directly from the various source systems in Bank A:

“So it’s not effective for us to go through the current account and the savings systems. Because if we go to current account and savings systems, then it’s a two ETL process.” (024)

Therefore, the utilisation of the CEISO capability has also allowed the accomplishment of supplementary benefits by allowing a business department to increase its turnaround time in acquiring the required information. The opportunity to leverage the regulatory IT repository had benefited the CRM department in the form of being cost-effective by not having to source the needed information directly from the core banking system and various fragmented systems in Bank A with different and inconsistent data formatting. Furthermore, when the repository is expanded to cover transactional information from more banking products55, the information made available to the CRM1 to attain supplementary benefits will also be more extensive and comprehensive [see Section 7.5.1].

Therefore, arising from the above discussions, the CEISO capability can be regarded as having the tendency to be utilised by the IT department during the post-establishment stage, in the attempt to ensure cost-effective IS operations for AML/CFT. Hence, arising from the usage of CEISO capability to ensure efficiency of organisation’s IT operations, a business department has been given a speedier access to a regulatory IT repository of cleansed transactional information need for its daily operations. The access was granted during the post-establishment stage, i.e. when the organisation AML/CFT IT solution has been fully operational.

The following evaluation table provides a structured understanding on how the usage of CEISO capability in influencing the occurrence of supplementary benefits, will likely lead to an improved competitive positioning for Bank A. As shown in the assessment provided below, as a whole, the CEISO capability does seemed to provide some form

55 To reiterate, the expanded number of banking products are; loans; credit cards; fixed deposits; auto finance; insurance; and stock broking. This will be over and above the current and saving accounts information that has been made available by the RSA1 system.
of business advantages to Bank A, due to its nature of possessing all the attributes being assessed:

Table 8-3: Business Advantages of CEISO Capability

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Definition</th>
<th>Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>Allow the implementation of strategies that enhance efficiency and effectiveness</td>
<td>Yes. The CEISO capability has provided value to Bank A in the form of faster turnaround time for the CRM department to acquire the needed information for the analysis in discovering marketing opportunities. This has therefore provided efficient and cost-effective operations for the CRM1 system, through the opportunity to leverage a regulatory IT repository.</td>
</tr>
<tr>
<td>Rarity</td>
<td>Allow exceptional usage of the capability that are not widely and similarly utilised by a huge number of organisations at the same time</td>
<td>Yes, the CEISO capability has exceptionally facilitated the efficiency and the increased turnaround time of a business department which is uniquely dependent on an information repository established for regulatory purposes, and subsequently be used to benefit the business of the organisation.</td>
</tr>
<tr>
<td>Appropriability</td>
<td>Ability to obtain returns accruing from the advantage</td>
<td>Yes. The CEISO capability has provided returns in terms providing efficient and cost-effective IS operations of the CRM1 system, by being allowed to access a regulatory IT repository of transactional information, rather than obtaining them directly from the various and fragmented source systems in Bank A.</td>
</tr>
</tbody>
</table>

8.3.4. Spanning Capabilities

It is interesting to note that none of the capabilities in this category, i.e. ISBP and ISPCM, has been found to be associated with the creation of supplementary benefits.

8.3.5. Additional Capabilities for Supplementary Benefits

In a nutshell, all the identified additional capabilities (i.e. CBP; BK and AIS) can be regarded as being associated with the creation of supplementary benefits. The
following sections will discuss in detail regarding these additional capabilities’ influence in the creation of supplementary benefits in Bank A.

a) Compliance-Business Partnerships (CBP)

It is worth reemphasising that some form of collaborations will generally exist between Compliance and business departments during the establishment of AML/CFT effort in the organisation. This is arising from the understanding that the information required for regulatory purposes is typically residing in various systems owned by business departments.

However, the ability to interact and obtain relevant information from business departments in Bank A has further revealed the possibilities of accomplishing supplementary benefits. In this regard, Bank A’s Compliance department had indeed been communicating with selected business departments on the possibility of obtaining the necessary information for regulatory purposes. The information, in this regard, is intended to act as an input for establishing customer risk profiling information in the regulatory system. Although it has been later decided that no information will be sourced from these departments, the interaction had somehow presented the opportunity for business departments to learn about the functionalities of the regulatory system.

The views and opinions of research participants will be able to explain the above statement further. In this regard, the Head of Analytics had highlighted that through this discussion process, the business departments have been made aware of the availability of risk profiling and other information that could benefit the business:56

“During the earlier part of implementation, initial phase, we called all the interested parties. ..... people from host, data warehouse, even CRM also, because initially what we were planning to do was actually take the

56 please note that this interview statement has been initially presented in Section 8.2.5(a). The statement has been reproduced in full in order to specifically showcase the interviewee’s last sentence that had revealed the notion of supplementary benefits detected by business departments. Also, it needs to be clarified further that the risk profiling information which had caught the interest from the business side, is specifically originating from the CRM department.
information from them for AML profiling. But along the way when they know that we are storing that information, and we are also running some sort of profiling, they become interested.” (017)

The above communication process can indeed be considered as an important occasion for the business. This is through the appreciation that business departments would not normally be consulted during the AML/CFT IT system’s development or establishment process. This can further be attributed to the situation where business departments are not regarded users of the system and therefore are not granted with an active role. Furthermore, they are typically not given access to most of the reports or information being generated, due to the confidentiality of information.

Most importantly, due to the contradicting priorities between business and compliance functions, Compliance department’s actions not directly enhancing banking business can be regarded as a norm. As related by the Head of National Leads, business departments in Bank A are typically considered as at the receiving end when it comes to the AML/CFT implementation. In addition, any requirements or measures being implemented by the Compliance department will need to be treated as directives and therefore will be obligated to be implemented:

“….. when it comes to the compliance, we were the one that are on the receiving end.” (030)

“So whatever things that they have developed, we are supposed to comply ….. their decision to proceed is not very much influenced by our requirements. So on our side, we are the one that will be able to leverage their system. It’s not that they have to oblige to our requirements.” (030)

Similar sentiment was also shared by Bank A’s Head of CRM. The interviewee had mentioned about the department being regarded as being at the tail end. Therefore, there was no motivation for the IT or Compliance departments to notify the CRM department about the development of an AML/CFT IT system:

“There is still a gap in terms of how the whole IT and Compliance departments so called work stream is happening. Because sometimes, some people are
been seen not part of that [system development], so you’re not made to know. Because maybe we are at the tail end.” (024)

Hence this nature of relationship seemed to provide one of the underlying reasons as to why business departments are generally not fully aware of the possible benefits of leveraging the AML/CFT implementation. Nevertheless, in Bank A, the session initiated by Compliance department intended to obtain information on customer profiling had resulted in the revelation of possible information that could be leveraged by the business.

From a different point of view, Bank A Compliance department’s practice of assisting the business in meeting regulatory requirements had also seemed to have a positive effect on the department’s sentiment in supporting the achievement of supplementary benefits. As previously mentioned in Section 7.6.1(b), through the tagline “Compliance Complementing Business”, Bank A’s Compliance department had attempted to project the idea of being a point of reference for business in relation to regulatory matters. Importantly, arising from one notable interview statement from the Head of AML/CFT and Compliance Strategy, the interviewee had explicitly acknowledged the idea of Compliance department being leveraged by business:57

“Because probably our spirit. We want to complement business. We have an open concept where we want business to leverage on us. The information, the system that we have in place.....” (034)

On the whole, the above statement has provided a testimony on the unique approach adopted by Bank A in assisting and facilitating compliance in the organisation, as well as its influence in accomplishing supplementary benefits through AML/CFT implementation.

The adopted approach and positive sentiment towards possible supplementary benefits as revealed above have provided one of the key justifications that can convincingly explain as to why the CRM department had been given permission to access the AML/CFT IT repository. As has been extensively explained in Section 7.5.1,

57 Please note that this interview statement has been first quoted in Section 7.6.1(b), but are being reproduced here for ease of reference.
the regulatory IT repository containing cleansed customer transactional information has indeed been leveraged by the CRM department to directly benefit banking business.

Importantly, Bank A’s receptive and accommodative nature in regard to leveraging AML/CFT efforts has provided good grounding for it to be considered as having higher inclinations to accomplish similar benefits within a structured and established business practices. As extensively presented in Section 7.6.1, by leveraging customer transactional information that had been considered as false alerts, the information can alternatively be used to consider pursuing any business enhancement activities with the identified customers. By doing so, Bank A will also be able to effectively mitigate the risk of inadvertently engaging with customers that may later turn out to be linked to ML/TF related activities.

Therefore, arising from the above discussions, the CBP capability can be regarded as having the tendency to be utilised by the Compliance department during the pre-deployment stage, in the attempt to obtain the necessary information from various business departments. Furthermore, through the usage of the CBP capability, the Compliance department adopted interactions and positive sentiment towards being leveraged by business, has assisted a business department to achieve supplementary benefits. The associated benefits, in this regard, can only be experienced during the post-establishment stage, i.e. when the organisation AML/CFT IT solution has been fully operational.

The following evaluation table provides a structured understanding on how the usage of CBP capability in influencing the occurrence of supplementary benefits, will likely lead to an improved competitive positioning for Bank A. As shown in the assessment provided below, as a whole, this capability does seemed to provide some form of business advantages to Bank A, due to its nature of possessing all the attributes being assessed:
Chapter 8: Analysis of Capabilities

Table 8-4: Business Advantages of CBP Capability

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Definition</th>
<th>Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>Allow the implementation of strategies that enhance efficiency and effectiveness</td>
<td>• Yes. The CBP capability has provided value through the speedier turnaround time for the CRM department to acquire the needed information. By accessing a regulatory repository, a cost-effective operation is being experienced by the CRM1 system. In addition, extended benefits will also be achieved when the information capacity in the repository is expanded in the future. • Furthermore, the capability also has the tendency to facilitate the likelihood of leveraging AML/CFT false alerts. This is used to initiate marketing initiatives that leverage specific incidences of a customer’s needs or demands.</td>
</tr>
<tr>
<td>Rarity</td>
<td>Allow exceptional usage of the capability that are not widely and similarly utilised by a huge number of organisations at the same time</td>
<td>• Yes. The CBP capability has exceptionally facilitated a unique dependency of the CRM department on a regulatory repository, and subsequently be used to directly benefit banking business. • In addition, the capability also has the tendency to exceptionally facilitate the likelihood of leveraging AML/CFT false alerts in a structured and established organisational practice. By doing the above, the organisation will be able to directly reduce the risk of inadvertently engaging with customers that may be associated ML/TF activities. Importantly, similar benefit is not available in other types of exception reporting or flagging mechanisms employed by the organisation [see also Section 7.6.1].</td>
</tr>
<tr>
<td>Appropriability</td>
<td>Ability to obtain returns accruing from the advantage</td>
<td>• Yes. The CBP capability has provided returns in the form of facilitating efficient and cost-effective IS operations through accessing the regulatory repository, as well as the information expansion when the capacity of the repository is enlarged. • This capability will also facilitate returns from the deployment of time-critical event-based marketing initiatives, by leveraging AML/CFT false alerts in a structured and established organisational practice.</td>
</tr>
</tbody>
</table>

b) Business Knowledge (BK)

Specifically viewing from the perspective of Bank A’s Compliance department for possessing understanding of business58, not only has the situation ensured the AML/CFT control measures being implemented are workable and practical, it has also

---

58 Possessing business knowledge from the perspective of the IT department will not be elaborated in this section as it has not been found to have influenced the creation of supplementary benefits for Bank A. The IT department has been regarded as one of the parties (i.e. besides Compliance department) that is actively involved in the AML/CFT IT system implementation process [see Section 8.2.5(b)]
seemed to contribute to the department being viewed as receptive and accommodative to the notion of supplementary benefits.

In this regard, it is sensible to assume that through firstly having adequate business understanding, only then will the circumstance allow for the Compliance department to be able to appreciate any possible business enhancements through AML/CFT implementation. In other words, it is reasonable to associate that through Bank A’s Compliance department adequate understanding of business, the department has been able to appreciate the added value that the organisation’s AML/CFT efforts would be able to offer to the business. This can be reflected through the comments made by the Head of Analytics, whom was seen to be very receptive on the idea of leveraging business benefits from compliance systems:

“I think that’s the only way to go actually ..... The beauty part of it is because in order to do for AML, you need to put so much effort, which can easily be used for other purposes. It’s really a waste if they are not doing that.” (002)

Importantly, possessing adequate knowledge of business can also be considered as one of the prerequisites in the ability to ascertain the accuracy of alerts being triggered by the AML/CFT IT system. In this regard, the review of alerted transactions should, among others, be based on comprehension of banking operations, as well as understanding organisation’s products and services, in determining whether the alerted transactions are considered as suspicious or otherwise.

Hence, the ability to possess business understanding can further be considered as one of the preconditions in the likelihood of achieving supplementary benefits through utilising AML/CFT false alerts. Furthermore, utilising customer information that has been regarded as genuine will also allow Bank A to eliminate the risk of unintentionally engaging with customers that may turn out to be involved with ML/TF activities. Bank A has indeed been regarded as having a higher tendency to potentially attain this type of supplementary benefits, within a structured and established organisational practice [see Section 7.6.1].

Therefore, arising from the above discussions, the BK capability can be regarded as having the tendency to be utilised by the Compliance department during the post-
Chapter 8: Analysis of Capabilities

*establishment* stage. This activity will be associated with assessing the accuracy and authenticity of alerted AML/CFT transactions. Furthermore, through the understanding of business, the identification of false alerts can indeed be done, and further be leveraged by a *business department* to achieve supplementary benefits. This type of benefit will be in the form of potentially deploying time-critical event-based marketing initiatives that leverage specific incidences of a customer’s needs or demands. The associated benefits, in this regard, can only be experienced during the *post-establishment* stage, i.e. when the organisation AML/CFT IT solution has been fully operational.

The following *evaluation table* provides a structured understanding on how the usage of BK capability in influencing the occurrence of supplementary benefits, will likely lead to an improved competitive positioning for Bank A. As shown in the assessment provided below, as a whole, this capability *does* seem to provide some form of business advantages to Bank A:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Definition</th>
<th>Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Value</strong></td>
<td>Allow the implementation of strategies that enhance efficiency and effectiveness</td>
<td>• <strong>Yes.</strong> The BK capability is considered as one of the preconditions for Bank A to appreciate and understand the value from leveraging AML/CFT false alerts to directly benefit banking business. Indeed, Bank A has been regarded as having a higher tendency to pursue time-critical event-based marketing efforts arising from these false alerts, within a structured and established organisational practice.</td>
</tr>
<tr>
<td><strong>Rarity</strong></td>
<td>Allow exceptional usage of the capability that are not widely and similarly utilised by a huge number of organisations at the same time</td>
<td>• <strong>Yes.</strong> The ability to ascertain whether alerted transactions are considered to be suspicious or otherwise using the BK capability will exceptionally influence the likelihood of Bank A to leverage these false alerts to directly benefit banking business. • Above all, the benefit of mitigating the risk of inadvertently dealing with customers associated with ML/TF is uniquely associated with AML/CFT false alerts. Therefore the ability to achieve this objective will not be similarly available in the organisation’s other exception reporting or flagging mechanisms.</td>
</tr>
<tr>
<td><strong>Appropriability</strong></td>
<td>Ability to obtain returns accruing from the advantage</td>
<td>• <strong>Yes.</strong> The BK capability will facilitate returns to Bank A’s through the probability of deploying time-critical event-based marketing initiatives that leverage specific incidences of a customer’s needs or demands.</td>
</tr>
</tbody>
</table>
c) Analytical and Investigation Skills (AIS)

This capability facilitates detailed analysis of transactional information and examination on alerted cases in the effort to mitigate the risk of ML/TF activities. Hence, from the perspective of business benefits, the AIS capability can be considered as one of the important prerequisite skills needed for the organisation to confirm whether the AML/CFT alerts are false positives, and therefore be an excellent source of information in the decision to deploy time-critical event-based marketing initiatives in Bank A. Furthermore, as explained in the preceding section, through the utilisation of customer information that has been regarded to be genuine will also allow Bank A to mitigate the risk of inadvertently dealing with customers that may turn out to be associated with ML/TF activities.

Elaborating this further, through the analysis and examination processes to confirm that an alert is not considered as suspicious, the organisation would be left with information that might indicate specific incidences of a customer’s needs or demands. As it will require the Compliance department good AIS capability in order to ascertain that a transaction is not suspicious, the resulting condition will also be able to reveal the various reasons as to why the transaction has been flagged off as suspected and subsequently, as the basis for it to be considered as false positives. Therefore, detailed understanding on the transaction through the AIS capability will allow Bank A to identify and subsequently leverage the information for business benefits once the transaction has been classified as valid.

Therefore, arising from the above discussions, the AIS capability can be regarded as having the tendency to be utilised by the Compliance department during the post-establishment stage. This activity will be associated with conducting comprehensive and thorough analysis, as well as examining suspicious cases in determining the accuracy and authenticity of alerted AML/CFT transactions. Furthermore, through the usage of this capability, the identification of false alerts can indeed be done, and further be leveraged by a business department to achieve supplementary benefits. This type of benefit will be in the form of potentially deploying time-critical event-based marketing initiatives that leverage specific incidences of a customer’s needs or
demands. The associated benefits, in this regard, can only be experienced during the *post-establishment* stage, i.e. when the organisation AML/CFT IT solution has been fully operational.

The following *evaluation table* provides a structured understanding on how the usage of AIS capability in influencing the occurrence of supplementary benefits, will likely lead to an improved competitive positioning for Bank A. As shown in the assessment provided below, as a whole, this capability *does* seem to provide some form of business advantages to Bank A:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Definition</th>
<th>Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>Allow the implementation of strategies that enhance efficiency and effectiveness</td>
<td>• Yes. The AIS capability is also considered as one of the preconditions for Bank A to appreciate and understand the value from leveraging AML/CFT false alerts to directly benefit banking business. Indeed, Bank A has been regarded as having a higher tendency to potentially pursue time-critical event-based marketing efforts arising from these false alerts, within a structured and established organisational practice.</td>
</tr>
<tr>
<td>Rarity</td>
<td>Allow exceptional usage of the capability that are not widely and similarly utilised by a huge number of organisations at the same time</td>
<td>• Yes. The ability to conduct comprehensive and thorough analysis, as well as examine suspicious cases using the AIS capability will exceptionally influenced the likelihood of Bank A to leverage AML/CFT false alerts to directly benefit banking business. • Above all, the benefit of mitigating the risk of inadvertently dealing with customers associated with ML/TF is uniquely associated with AML/CFT false alerts. Therefore, the ability to achieve this would not be similarly available in the organisation’s other exception reporting or flagging mechanisms</td>
</tr>
<tr>
<td>Appropriability</td>
<td>Ability to obtain returns accruing from the advantage</td>
<td>• Yes. The BK capability will facilitate returns to Bank A’s through the probability of deploying time-critical event-based marketing initiatives that leverage specific incidences of a customer’s needs or demands.</td>
</tr>
</tbody>
</table>

8.3.6. **Summary and Conclusion**

Out of the six capabilities suggested by Wade and Hulland (2004) that were found to have influenced compliance benefits [see Figure 8-4], only *three* capabilities (i.e. ERM;
Chapter 8: Analysis of Capabilities

ISI; and CEISO) have been further considered to assist Bank A in attaining supplementary benefits from AML/CFT implementation. Meanwhile, in relation to the additional capabilities, all three capabilities (i.e. CBP; BK; and AIS) are similarly regarded to have facilitated the achievement of this objective. Therefore, as a whole, only six out of nine capabilities (i.e. including the supplementary) found to influence compliance benefits, have been regarded to have further influenced supplementary benefits in Bank A [see Appendix XI for an overview on the analysis of capabilities].

The smaller set of capabilities influencing supplementary benefits (i.e. six) as compared to compliance benefits (i.e. nine) should be appreciated from the perspective of the earlier statements in Sections 8.2.1 and 8.3.1. In this regard, given that the expected regulatory deliverables are similarly anticipated from each institution within the banking industry, the capabilities facilitating the realisation of these deliverables (and compliance benefits) would therefore be equally experienced by all organisations. Nevertheless, since only Bank A has solitarily been seen to (or will) accomplish the identified set of supplementary benefits arising from the deployment of regulatory IT solution [see Chapter 7], therefore it can be acknowledged that capabilities in Bank A had indeed been utilised differently from other organisations. In this regard, only a selected (and smaller set) of Bank A’s capabilities were found to be used beyond the needed basic activities of AML/CFT implementation. Therefore, the usage of these capabilities can thus be regarded as not being commonly experienced by all organisations, as their utilisation was seen to be over and above their fundamental usage for achieving compliance benefits.

The above situation can also be explained through the viewpoint of existing literature. As suggested by Doherty (2013), one of the key principles and practices of benefits realisation management through leveraging organisation’s IT investments is in effect a journey, and therefore, should not be considered as merely a destination. Active management of benefits over the IT solution’s operational lifespan is critical (Doherty, 2013, Leonardi, 2007). Fitting this principle into the specific context of this research, expected regulatory deliverables can therefore be regarded as what organisations wish to hurriedly achieve (i.e. a destination), and facilitated through the usage of relevant capabilities. Instead, the utilisation of some capabilities in achieving the
anticipated deliverables (and thus compliance benefits) can indeed be broaden and continued further, in the attempt to experience possible supplementary benefits (i.e. the journey).

The following Figure 8-5 graphically illustrates this principle from the viewpoint of the associated capabilities discovered in the research. The line representing the usage of the six capabilities facilitating supplementary benefits can therefore be regarded as continuously shifting in order to manage (and probably discover new) supplementary benefits arising from the deployment and operationalisation of AML/CFT IT solution:

<table>
<thead>
<tr>
<th>ERM</th>
<th>MR</th>
<th>ISI</th>
<th>ISD</th>
<th>CEISO</th>
<th>ISBP</th>
<th>CBP</th>
<th>BK</th>
<th>AIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance Benefits</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 8-5: Extended Usage of Capabilities Facilitating Supplementary Benefits**

Moving the discussion to the assessment on their possibly to improve the competitive positioning of Bank A, only five (i.e. ISI; CEISO; CBP; BK; and AIS) out of these six capabilities highlighted in the preceding paragraphs seemed to exhibit this quality. Therefore, it can be further regarded that, while it may be sensible to conceive that only selected capabilities will tend to facilitate supplementary benefits, not all of these capabilities will necessarily influence organisation’s competitive positioning in a positive and constructive manner. This situation can also be reflected through the
suggestions in the literature, which had highlighted that only a few superior capabilities owned by organisations may allow them to outperform others (Day, 1994). Moreover, it is useful to likewise note that the capabilities seen to facilitate supplementary benefits may arise in both stages of AML/CFT implementation. Importantly, most benefits may also emerge through the usage by Compliance or IT departments, or both, to firstly address the needed compliance activities. This particular situation can be attributed to the understanding that the priority adopted by Bank A is still seen to be principally focusing on ensuring compliance [see also Section 7.6.1(b)]. Only after full implementation of the regulatory initiatives, will the situation allow for supplementary benefits to be experienced by related business departments in the organisation, as depicted in Figure 8-6:

![Figure 8-6: Relationships - Department, Stage, Capability & Supplementary Benefits](image)

<table>
<thead>
<tr>
<th>ERM</th>
<th>ISI</th>
<th>CEISO</th>
<th>CBP</th>
<th>BK</th>
<th>AIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leverage Identification &amp; Background Information</td>
<td>Leverage Riskiness Information</td>
<td>Leverage Opportunity to be Selective</td>
<td>Leverage Fraud Functionalities</td>
<td>Leverage Regulatory IT Repository</td>
<td>Leverage Time-Critical Event-based Information</td>
</tr>
</tbody>
</table>

ERM: External Relationship Management  
ISI: IS Infrastructure  
CEISO: Cost-Effective IS Operations  
CBP: Compliance-Business Partnerships  
BK: Business Knowledge  
AIS: Analytical and Investigation Skills

8.4. CONCLUDING REMARKS

In conclusion, this chapter have provided meaningful insights and justifications on the various capabilities that were considered to have influenced or facilitated the
attainment of compliance and supplementary benefits. The presentation on analysis of capabilities is critical to this research, as it has allowed for the identification of capabilities needed to enable comply with the numerous required activities, as well as to directly benefit the business of the organisation.

Moving forward, the thesis will present an overall discussion and conclusion for the research. Importantly, it will also offer an updated framework, based on the insights that have been obtained throughout the analysis.
Chapter 9
Discussion and Conclusions

9.1. INTRODUCTION

This final chapter will present an overall summarisation of the results of the analyses, as well as the conclusions that can be derived from the research. It will commence by outlining the summary of key findings, in relation to the research objectives outlined in Chapter 3. Subsequently, the chapter will provide the overall discussions based on the outcomes of the research. Furthermore, arising from the understanding and insights obtained throughout the analysis, a revised framework for assessing possible benefits arising from regulatory IT implementations, will be presented. The revised framework, in this regard, is better suited to discover supplementary benefits from the need to comply with regulatory requirements. In addition, this chapter will also be presenting the implications of the research, acknowledging the limitations of the study; as well as identifying the opportunities for future research, before it is summarised by the concluding remarks section.

9.2. SUMMARY OF KEY FINDINGS

The summary of main findings will be presented in relation to the four research objectives that have driven the research, as outlined in Section 3.3. The approach to bring together the all the research findings into one section will definitely be helpful in putting the whole discussion into perspective, i.e. from the overall context of the research.
9.2.1. First Research Objective

**RO1a:** To understand the overall approaches and mechanisms by which banking institutions translate the regulators’ requirements into functional specifications for their compliance system;

**RO1b:** To understand and appreciate instances of compliance benefits arising from banking institutions meeting the regulatory requirements.

The first research objective comprises of two goals that aim to assess the possible value arising from basic compliance activities. The first part of the objective was intended to appreciate banking institutions’ approaches and mechanisms for translating regulatory requirements into functional specifications, and thus meeting the expected deliverables and avoiding regulatory penalties. Meanwhile, the second part was aimed at appreciating the accomplishment of compliance benefits arising from this type of activity.

In specific relation to the first part of this research objective, i.e. **RO1a**, there was lack of evidence to suggest that the sample organisations were utilising predetermined methodologies; structures; or templates, which can be considered as a basic approach and mechanism to regulatory compliance. Addressing regulatory requirements were, in effect, seen to exhibit no structured or standardised mechanisms, as they are particularly regarded as an ad-hoc activity. Hence, the envisaged increase in efficiency or effectiveness, and achievement of cost savings through compliance efforts suggested by the literature, could not be fully substantiated in these organisations. Furthermore, arising from the absence of overlapping requirements, cost savings through concerted compliance efforts to address multiple requirements that are of similar in nature were also not discovered.

In effect, the primary intention in these organisations’ regulatory compliance activities was not aiming to reduce cost of compliance arising from the adaptation of structured and standardised efforts. It was revealed that ensuring compliance to the requirements is always a priority. The sense of urgency and the criticality to be compliant were detected in most interviews conducted, due to the potential adverse implications from the regulatory authority.
Meanwhile, in relation to the second part of this research objective, i.e. RO1b, it is interesting to note that compliance benefits arising from the sample institutions meeting the regulatory requirements have been detected. However, arising from the outcome from RO1a, these detected benefits could not be associated with any structured and standardised efforts undertaken by these organisations to minimise the cost of compliance, or increase the associated efficiency or effectiveness. Rather, they arise from the resulting condition subsequent to the accomplishment of expected regulatory deliverables. In other words, only through attaining the expected deliverables had the situation allowed these organisations to experience compliance benefits.

In relation to the process of discovering the compliance benefits, they were derived from the key themes detected from the analysis of interview data, as well as, the insights obtained from a comprehensive review of the associated regulatory requirements. Importantly, they were identified arising from their association with organisations’ efforts to basically meet the requirements. This is regarded as being done without the implementation of extended activities, considerations or changes that could directly benefit banking business.

A total of fifteen compliance benefits were discovered by the research. Besides four benefits that were being categorised as reputational compliance benefits, the remaining eleven can be associated with four additional categories. These categories were pertaining to benefits arising from verification; monitoring; and categorisation of customers’ information; as well as from the decision to computerise AML/CFT related compliance activities.

9.2.2. Second Research Objective

RO2a: To understand the approaches and mechanisms by which banking institutions take into account other influences, when responding to regulators’ requirements;
RO2b: To understand and appreciate instances of supplementary benefits that directly benefit banking business, arising from banking institutions decision to leverage compliance activities.

The second research objective also comprises of two goals, arising from extended compliance activities. The first part was intended to appreciate any instances of banking institutions taking deliberate efforts to implement supplementary business related activities when responding to regulatory requirements. Meanwhile, the second part was aimed to appreciate any accomplishment of supplementary benefits that positively benefit banking business arising from the decision to leverage compliance activities.

With regard to the first part of this research objective, i.e. RO2a, there was also little evidence to suggest that deliberate attempts to incorporate extended activities, additional considerations or optional changes were carried out by the sample organisations when responding to regulatory requirements. In effect, these organisations were seen to typically aiming to meet the minimum regulatory requirements, in order not to be imposing unnecessary restrictive measures to the business.

As had been mentioned in the discussion pertaining to RO1a, ensuring successful compliance has always been seen as the overriding principle. A sense of urgency and the crucialness to be compliant were continuously detected during the interviews. This situation can be particularly attributed to the understanding that deployment of AML/CFT IT solution was typically the responsibility of Compliance department. Therefore, it is understandable that the principal motivation to establish these systems were intended to primarily address compliance objectives, and not to deliberately consider incorporating extra or optional activities.

In relation to the second part of this research objective, i.e. RO2b, it is important to note that instances of supplementary benefits have indeed been detected. However, arising from the outcome from RO2a, these discovered benefits could not be associated with the sample organisation’s deliberate incorporation of extended activities, additional considerations or optional changes during regulatory compliance
efforts. As the detected benefits had not arise from the extended compliance activities suggested by the literature, they are seen to instead be mainly linked to possible alternative usage of compliance information that is being gathered; processed; and generated by regulatory IT system upon successful implementation.

In relation to the process of discovering the supplementary benefits, they have been detected through the analysis of the interview data, as well as, from a comprehensive review of related regulatory requirements. However, the analysis had also significantly capitalised on the extensive discussion of compliance benefits in order to provide the discovery and deeper understanding on supplementary benefits. Therefore, it is essential to note that acknowledging compliance benefits can thus be regarded as one of the qualifying conditions for supplementary benefits to be appreciated and experienced. Indeed, a connection between compliance and supplementary benefits has been established by the research [see Figure 7-1].

A total of six supplementary benefits have been discovered by the research. These benefits can be classified according to five categories. These categories were pertaining to benefits arising from customer information; customer selection; fraud mitigation; information repository; as well as event-based information. The smaller number of detected supplementary benefits (i.e. as compared to compliance benefits in RO2b) can be explained through the perspective that these benefits were in effect, not the expected outcomes of a regulatory driven IT implementation. Furthermore, not all instances of detected compliance benefits mentioned in RO2b will necessarily imply supplementary benefits to be experienced, due to various reasons, including their possible infeasibility and impracticality.

9.2.3. Third Research Objective

RO3: To explore and understand the banking institutions’ portfolio of IS capabilities that are being utilised to facilitate both compliance and supplementary benefits.
Chapter 9: Discussion and Conclusions

The third research objective aim to explore and understand the portfolio of IS capabilities that have assisted banking institutions to attain expected compliance benefits. In addition, it is also intended to appreciate the list of IS capabilities that have possibility facilitated the achievement of supplementary benefits.

Overall, the analysis has provided empirical evidence to indicate that not all eight capabilities suggested by Wade and Hulland (2004) has been found to be useful for the sample organisations to achieve compliance benefits through AML/CFT IT implementation. In this regard, two capabilities, i.e. ISTS and ISPCM, were not regarded as having any influence in the organisations’ efforts to achieve the detected compliance benefits initially mentioned in RO2b.

In addition, the outcome of the analysis had also importantly suggested several extra capabilities in achieving a similar objective. In this regard, these extra capabilities have been classified as additional capabilities, since they are not part of the list of key capabilities originally suggested by Wade and Hulland (2004). The additional capabilities detected are CBP; BK; and AIS. It is important to note that these additional capabilities might only be useful within the effort to implement AML/CFT initiatives, and further aid in achieving compliance benefits. Furthermore, they were also viewed as organisational typed capabilities, as opposed to being regarded as technical typed capabilities.

Together with the initial list of six capabilities suggested by the literature (i.e. ERM; MR; ISI; ISD; CEISO; and ISBP) and the three additional capabilities mentioned above, a total of nine capabilities have been regarded as playing a significant role for these organisations in achieving compliance benefits. Therefore, these capabilities can also be regarded as the set of key capabilities critically required to meet AML/CFT requirements, and further assist in experiencing the associated compliance benefits.

In addition, while some capabilities were seen to be more useful or consistently playing a critical role in a particular stage of the implementation (i.e. pre-deployment; or post-establishment), there are instances where other capabilities (i.e. particularly CBP; and BK) were being considered to be required in both stages. A similar principle also applies to the department that was seen to have the tendency to utilise these
capabilities. In this regard, while some capabilities may have higher inclinations to be separately used by the Compliance or IT departments, both departments have been seen to simultaneously utilising the ERM and BK capabilities in the pre-deployment stage of AML/CFT IT implementation [see Figure 8-4].

In specific relation to the list of IS capabilities associated with supplementary benefits, only six out of the nine capabilities identified earlier (i.e. in relation to compliance benefits) were found to have further assisted an organisation in experiencing supplementary benefits. In this regard, only three capabilities (i.e. ERM; ISI; and CEISO) suggested by Wade and Hulland (2004) and all three additional capabilities (i.e. CBP; BK; and AIS) have been considered to have assisted Bank A in attaining supplementary benefits from AML/CFT implementation.

It is useful to note that the usage of capabilities relating to supplementary benefits were mainly associated with two key departments (i.e. Compliance and IT). As these departments were considered as having an active role in the deployment and establishment of AML/CFT IT systems, they have been seen to utilise the capabilities to firstly address the needed compliance activities. Only after full implementation of the regulatory initiatives, has the situation allowed for supplementary benefits to be experienced by related business departments in the organisation [see Figure 8-5].

Furthermore, it is essential to note that the usage of the capabilities related to supplementary benefits were also partly seen from the perspective of Compliance department, and thus were not only confining to the utilisation by IT function. This situation is due to the understanding that the AML/CFT implementation efforts are primarily driven by regulatory requirements. Therefore, since they will be mainly managed or overseen by the Compliance departments, some of the associated capabilities have more propensity to be utilised by this particular department.

Furthermore, as acknowledged in Section 3.4.2, the inside-out classification of capabilities is also seen to be more inclined towards emphasising the technical competencies aspects of IT. Meanwhile the rest of the categorisations (i.e. outside-in and spanning) tend to lean towards the perspective of a broader organisational general competencies demonstrated by the IT functions (as well as, in this particular
Chapter 9: Discussion and Conclusions

case, any other related departments such as the Compliance function). Moreover, in further supporting the above proposition, it may also useful to revisit the suggestion by Bharadwaj (2000). In this regard, the author has suggested that IS capabilities should be defined as a firm’s ability to deploy IT-based resources together with what are being regarded as non-IT resources and capabilities.

9.2.4. Fourth Research Objective

RO4: To investigate how through the utilisation of capabilities in realising compliance benefits and supplementary benefits, a financial institution might improve its competitive positioning.

The final research objective aims to gain insights into whether the attainment of expected compliance benefits through by the utilisation of associated capabilities, have indeed positively influenced organisation’s competitive positioning. Similarly, it is also aimed to explore whether the attainment of supplementary benefits through the usage of relevant capabilities have likewise provided a similar influence.

As has been mentioned in Section 8.3.1(v), the assessment of competitive positioning from the perspective of capabilities relating to compliance benefits was no longer deemed as a sensible approach. This is arising from the outcome for RO1a that had suggested the lack of evidence to support an earlier assumption made in Section 3.3.4. It was envisaged earlier that compliance benefits could also have the ability to influence the organisation’s competitive positioning through uniquely deploying efficient and effective compliance activities, and reducing compliance cost. Since the results for RO1a has not supported the envisaged increase in efficiency or effectiveness, and achievement of cost savings, the role of capabilities related to compliance benefits in influencing organisation’s competitive positioning are no longer a viable path that is worth pursuing.

Nevertheless, from the perspective of capabilities associated with supplementary benefits, the analysis has provided empirical evidence to suggest that the achievement of supplementary benefits through the usage of the associated
Chapter 9: Discussion and Conclusions

capabilities had influenced an organisation’s competitive positioning. However, it is important to note that only five (i.e. ISI; CEISO; CBP; BK; and AIS) out of the six capabilities (i.e. excluding ERM) had exhibited the quality of influencing competitive positioning. Therefore, evidence has shown that not all capabilities related to supplementary benefits will necessarily influence organisation’s competitive positioning in a positive and constructive manner.

It is also important to note that the positive influence on Bank A’s competitive positioning, arising from the usage of these five capabilities in achieving supplementary benefits, was measured by assessing the attributes suggested by Wade and Hulland (2004) [see Sections 3.4.3 and 8.3.1(iv)]. Therefore, the relationships between capabilities and competitive positioning for Bank A in this regard, were inferred or deduced from the detailed insights obtained throughout the study. The approach was taken arising from the appreciation that none of the interview respondents in Bank A had explicitly highlighted or directly stated that the organisation’s competitive positioning had been positively influenced through the implementation of its AML/CFT IT system. This situation can also be attributed to the general understanding that the deployment of regulatory IT systems were usually not intended to directly benefit organisation’s business, or improve organisational revenue [see Section 1.2].

9.2.5. Overall Summary

From an overall perspective, it is important to further reflect on some the above findings and contrast these with the relationships that had been hypothesised in the research framework [see Section 3.4.1]. In this regard, it can be confirmed that some of the predicted relationships could not be fully substantiated by the research. On the other hand, one unexpected relationship has interestingly been uncovered by the analysis.

With regard to the relationship that was not supported by evidence, it has been ascertained that the discovery of compliance benefits were not attributed to any approaches and mechanisms aiming to increase the effectiveness and efficiency of
regulatory activities. Rather, these types of benefits were uncovered throughout the analysis of interview data, and insights from a detailed review of relevant documents. In this regard, these benefits were seen to be partly arising from the accomplishment of expected regulatory deliverables, and therefore not influenced by any specific regulatory approach or mechanism. Organisations were seen to be able to experience compliance benefits primarily through firstly attaining the associated required deliverables.

Similarly, the suggestion to incorporate extended activities, additional considerations or optional changes was also not able to be related with the discovery of supplementary benefits. Instances regarded as supplementary benefits were detected via the analysis of primary data, and importantly capitalising on the knowledge regarding compliance benefits. Through the appreciation of similar requirements that have been influencing compliance, as well as supplementary benefits, relationship between these two types of benefits has indeed been established [see Figure 7-1]. Therefore, the appreciation on compliance benefits can also be regarded as partly causing supplementary benefits to be experienced by organisations.

This relationship between compliance benefits and supplementary benefits is unexpected and has not being acknowledged in the research framework [see Section 3.4.1]. From the initial review of the literature, supplementary benefits were envisaged only to be obtained from organisation’s efforts to include optional business considerations within regulatory driven IT implementations. Since this deliberate activity was not found, the instances of detected supplementary benefits tend to be more inclined to be associated with the resulting condition of firstly complying with regulatory requirements, and further be leveraged to benefit organisation’s business directly.

9.3. RESEARCH CONTRIBUTIONS

In relation to the research contributions, the knowledge that this study is offering can generally be divided into two broad areas. The first area of contribution is regarded as
directly arising from the various insights obtained from the deployment of this research. Meanwhile, the second area of contribution is in the form of a revised framework that the study is proposing, which has been crafted mainly from the overall understanding and general appreciation of the research findings. The following sections will discuss these two general areas of research contributions further.

9.3.1. Contributions Arising from Research Findings

Arising from the many useful findings and insights presented in this thesis, it is possible to discern a number of significant new contributions that this study has made to the extant research literature. One of the most significant contributions, arising from the empirical evidence presented in this thesis, relates to the relationship between the activities undertaken to meet regulatory requirements and the resultant realisation of benefits to the host organisations. More specifically, although regulatory compliance activities are commonly regarded as a cost of doing business that generally burdens the organisation (e.g. Walter and Rolf, 2005, van Oosterhout et al., 2006, Elliehausen, 1998, Garneau and Shahid, 2009, Gable, 2005, Pakravan, 2011), this study has provided real-life testimony to show that this situation is not always the case. The various expectations for abiding with AML/CFT requirements can, in effect, be effectively evaluated from the perspective of enhancing organisational performance, through the leveraging of the various informational assets that have been made available, due to regulation. Such benefits have been classified as being either compliance benefits or supplementary benefits.

More specifically, this study has explicitly outlined the various compliance benefits that have been experienced by the case study organisations, through their efforts to simply meet AML/CFT regulatory requirements, and thus avoid any associated penalties. Whilst prior studies may have intimated that the introduction of IT to facilitate an organisation’s compliance with regulatory requirements may be a sensible and positive strategy (e.g. Lurie, 2004, Volonino et al., 2004, Luthy and Forcht, 2006), this study is the first to have explicitly articulated a taxonomy of compliance benefits, in any regulatory context. Consequently, the identification of fifteen distinct
compliance benefits to be leveraged from the introduction of AML/CFT systems, is an important new contribution to the literature.

Whilst many previous studies have highlighted the possibility of using customer-related information to leverage improvements in competitive positioning (e.g. Kozak, 2007, Subbulakshmi, 2012, Foss and Stone, 2002), no previous studies have explicitly attempted to identify the types of customer-related benefit that might be leveraged from the introduction of regulatory systems. Consequently, this study makes another important contribution by identifying and describing the specific types of customer-facing, supplementary benefits, which financial services organisations might leverage from the implementation of AML/CFT technologies. More specifically, six distinct types of supplementary benefits, which might arise from the implementation of AML/CFT IT systems within banking institutions, have been successfully identified.

By so doing, the study has not only managed to place the spotlight on possible benefits arising from regulatory led IT investments, but has also successfully identified and differentiated these two types of benefits, which seemed to have not been attempted by IS researchers in any previous studies. Indeed, value research focusing on mainstream IT systems (e.g. Barua et al., 1995, Mahmood and Mann, 2005, Peppard et al., 2000, Doherty and Terry, 2009, Mahmood and Mann, 1993, Melville et al., 2004) is abundant, yet, research on compliance systems has been given far less emphasis by IS researchers. Hence, while it is sensible to consider that regulatory IT implementations are typically not intended to directly benefit business, the evidence presented in the study has suggested that similar discussion within the IS domain should not be entirely ignored. The needed research attention on regulatory IT investments can be further appreciated through their financial significance. Indeed, it has been reported that banking institutions’ global IT spending (as well as on operations) in order to comply with AML/CFT requirements is estimated to reach USD5.8 billion in 2013 (Adams, 2012). Therefore, since business executives had always continued to question and seek evidence of their substantial investments in IT (e.g. Chang and King, 2005, Mahmood and Mann, 2005), research focus on these financially significant IT investments that are being used for regulatory purposes need to be similarly emphasised by IS researchers.
Moving the discussion to the perspective of capabilities, the study has also managed to effectively ascertain what can be regarded as the set of key capabilities for organisations to achieve compliance benefits. In this regard, the study has found that only six, out of eight capabilities suggested by Wade and Hulland (2004), were helpful to achieve compliance benefits through AML/CFT IT implementation. This situation is over and above the three additional capabilities that were seen to be similarly important to achieve the identified compliance benefits for the sample organisations. Importantly, as it has been suggested that organisations’ survival are being influenced by their IT capabilities (e.g. Bharadwaj et al., 1999), the same principle may also be applied to the capabilities being associated with regulatory compliance. In this regard, it is therefore envisaged that this set of capabilities will be critical for any organisations intending to avoid any adverse repercussions arising from the lack of compliance with AML/CFT regulatory requirements, and further to experience the associated compliance benefits [see Section 8.2].

Furthermore, the study had also successfully pinpointed the set of capabilities which can be extended to facilitate the achievement of supplementary benefits [see Section 8.3]. In this regard, only three capabilities suggested by Wade and Hulland (2004) and all three identified additional capabilities have been considered to have assisted Bank A in attaining supplementary benefits from AML/CFT implementation. Moreover, the study had also effectively established and confirmed the list of capabilities that are regarded to be influencing organisation’s competitive positioning. As revealed by the analysis, only five of the previously mentioned capabilities had exhibited the quality of influencing competitive positioning of Bank A in a positive and constructive manner. Therefore, the study has provided evidence and further support on the growing evidence suggesting the superiority in capabilities deployment as being considered a source for organisation’s competitive advantage (e.g. Wade and Hulland, 2004, Day, 1994, Christensen and Overdorf, 2000, Bharadwaj, 2000, Santhanam and Hartono, 2003).

It is important to note that since IT value studies on regulatory driven IT systems appeared to be lacking in the literature, information relating to capabilities associated with the achievement of compliance benefits; supplementary benefits; as well as
influencing organisation’s competitive positioning are also seemed to be deficient. Hence, another contribution arising from this study, is regarding the definition of capabilities that match with the characteristics of regulatory compliance. The definition of these regulatory related capabilities was created based on the ones suggested by Wade and Hulland (2004). Therefore, with the availability of capabilities specifically associated with regulatory compliance, any future research projects having similar motivation should effectively leverage the knowledge that has already been made available. This situation will be over and above to the list of additional capabilities and their associated definitions that have been identified arising from the outcome of this study.

9.3.2. Contribution in the Form of a Revised Framework

In a nutshell, the undetected relationships, as well as the discovery of a new affiliation that have been discussed in Section 9.2.5 had all pointed towards the unsuitability of the existing framework in discovering potential business benefits from regulatory IT implementations. Hence, arising from the this particular understanding, as well as other insights obtained from the analysis of data, the study will be introducing a revised framework that is regarded to be better suited in facilitating the accomplishment of this particular objective. It is important to note that the revised framework was not solely derived from the appreciation and understanding obtained through the analysis of research data. It was also effectively based on an additional review of the associated literature arising from the new information gathered by the research. Therefore, this particular framework can be further regarded as having emerged from the appreciation of empirical data, as well as be based on insights obtained from the existing knowledge, particularly pertaining to the related areas of interest. The following Figure 9-1 summarises the discussion by presenting the key phases that had contributed to the realisation of the revised framework:
In addition, by considering this revised framework as one of the research contributions, the effort will also matches with the theoretical foundations that have been adopted by the research. As mentioned in Section 4.5.2, the research has inclinations to adopt two key concepts from the grounded theory for its approach of analysing data. One of the key concepts that has been observed is in effect highlighting the motivation and intention to develop a theory out of the data. Similarly, from a philosophical standpoint [see Section 4.2], it has also matched with the inductive perspective being utilised by this research. The inductive orientation of social research likewise suggests that a theory would be typically devised, or being an outcome to research adopting the qualitative approach.

The rest of the discussion on the revised framework will be based on Figure 9-2, which has visually illustrated, as well as showcased the associated direction of causality.
a) Framework on Assessing Business Benefits of Mandatory IT Implementations

![Diagram](relationship_between_compliance_and_supplementary_benefits)

Figure 9-2: Framework on Assessing Business Benefits of Mandatory IT Implementations

It is essential to appreciate at this juncture regarding the two key guiding principles that have provided the underlying motivation and rationale for the design of the revised framework. The key guiding principles are as follows:

1). Initiation of Assessment Upon Full Deployment

In relation to the first guiding principle, the framework considers that any effort to assess possible business benefits from regulatory IT implementations is to be done once the compliance system has been successful implemented. Attempting to assess potential benefits when regulatory IT systems are yet to be fully operational may run the risk of not obtaining full cooperation from the associated parties.

Indeed it has been discovered that organisations would tend to comply with regulatory requirements without delay due to the possible adverse implications for
being regarded as lacking in compliance. In effect, literature has also suggested that when considering IT initiatives arising from regulatory requirements, organisations often have limited discretion and inflexible implementation timeframe (Krell et al., 2011, Joshi and Pant, 2008). Therefore a thorough feasibility analysis providing justifications for the investment [i.e. ex-ante evaluation (Marthandan and Tang, 2010)] would not be beneficial or necessary to facilitate investment decision (Joshi and Pant, 2008). For instance, compliance driven by fear is said to be common in the implementation of anti-money laundering measures, and organisations tend to treat regulatory recommendations as directives (Demetis and Angell, 2006).

It can therefore be regarded that evaluation of possible benefits from regulatory driven IT systems is best to be done once the system has been successfully implemented, i.e. from ex-post or post-implementation orientation. However, it is essential to further note that existing benefit evaluation techniques for general IT system implementations in the extant literature may not entirely be suitable to assess the possible benefits generated from compliance systems. One of the ways to measure the success of a typical IT system implementation from ex-post perspective is evaluated from the principles of comparing projected benefits against realised outcomes (Marthandan and Tang, 2010, Gable et al., 2008). In contrast, the development of compliance systems can be regarded as importantly not being premised on the assumption of benefits\(^{59}\), or even adopting typical business justifications. Again, this situation is due to the fear of repercussions for not meeting regulatory authority’s expectations, and therefore the typical assessment approach could not be utilised as practical comparisons are not possible.

Furthermore, as seen from the analysis, it is unlikely that system development process for compliance systems will attempt to incorporate business requirements. Hence, the idea of incorporating business requirements in a mandatory system

---

\(^{59}\) As initially highlighted in Section 6.1.1, organisations are not regarded as being intentionally planning to achieve compliance benefits (or even supplementary benefits) through the implementation of regulatory IT systems. They were instead seen as more aiming to be compliant with the requirements, and primarily to avoid adverse repercussions from the regulatory authority. Therefore, clear statements of possible achievable benefits that can be used for the above post-implementation review will not be typically available.
implementation (e.g. Garcia, 2004, Krell and Matook, 2009), may not be a useful avenue to assess the potentiality of business benefits from compliance systems implementations.

Therefore, as a whole, and inspired by the above discussions, the revised framework will be focusing to assess the potential benefits once all the regulatory expectations have successfully been met. In addition, the associated assessments will be using an approach that has been uniquely adopted for regulatory driven IT systems.

\textit{ii). Benefits Evaluation Utilising Qualitative Perspectives}

Moving on to the second guiding principle, many IT investment initiatives for the purpose of meeting regulatory requirements has been regarded as not allowing easy measurement of benefits (Joshi and Pant, 2008). Therefore, as initially highlighted in Section 4.3.1, since compliance systems development is not premised on benefit realisations or typical business justifications, the measurement of benefits from the quantitative perspective would be inherently challenging due to the absence of initial measurement indicators.

Arising from the above, the framework will adopt a principle that potential benefits from regulatory driven IT systems are to be assessed from the qualitative lens instead. The rationale for this approach is primarily due to the appreciation that many benefits derived from IT are primarily intangible, such as improved customer service, better flexibility and superior product quality (Joshi and Pant, 2008, Bharadwaj et al., 1999). Correspondingly, it is likewise anticipated that benefits from compliance systems would also predominantly be intangible. Nevertheless, the reason to particularly adopt this approach should also essentially be attributed to the unique nature of these systems. In this regard, these systems are not designed to provide business benefits in the first place, or even aimed to impact organisation’s bottom line in a positive manner. Therefore, drawing conclusions from the quantitative orientation could be viewed as a more complicated route (although should not be regarded as entirely unachievable).
Chapter 9: Discussion and Conclusions

The following presentation will discuss and justify the revised framework further by following the sequence of assessment suggested by the direction of causality in Figure 9-2. The discussion, in this regard, would be more inclined to showcase how possible business benefits from regulatory IT implementations can practically be detected and evaluated using the framework:

i). The assessment of possible business benefits from regulatory IT systems is to be commenced through the appreciation of the attainable **compliance benefits**. The identification of compliance benefits, in this regard, should be guided or driven by the various regulatory deliverables that organisations are required to accomplish. Therefore, these regulatory deliverables can be regarded as a primary source of information for the framework, as they are being considered to be the key motivation for deploying regulatory compliance activities. Hence, by appreciating what needs to be delivered, compliance benefits can be identified from the resulting condition, subsequent to the accomplishment of the deliverables;

ii). The assessment of possible compliance benefits is to be done in a structured and systematic manner. As can be seen throughout the analysis of compliance benefits in Chapter 6, a **summary table** had been used at the end of each discussion for each particular compliance benefit that had been identified. In this regard, the factors used for the assessment have been inspired by the suggestions made by Chan (2000), i.e. pertaining to; **what; why; where; when; who; and how**. The reason to adopt this approach is to assist in clarifying the detected compliance benefits. In addition, it is also to provide clear guidance during the necessary discussions with relevant parties when the feasibility of business benefits is further evaluated, as well as the facilitate the possibility of uncovering more supplementary benefits;

iii). The assessment of **capabilities** regarded to have influenced the realisation of compliance benefits is to be done only after the compliance benefits have been adequately identified. The six capabilities obtained through the work by Wade

---

60 Chan (2000) suggests that a set of questions should be asked on IT value research in determining the value provided by IT investments, i.e.; **why; where; when; how; and to whom**. These questions are to be asked over and above to the question of **what**, which has been regarded as a common approach utilised by IS researchers.
Chapter 9: Discussion and Conclusions

and Hulland (2004) and the three additional capabilities identified by the research can be used as a basis for the assessment. Furthermore the identification of relevant capabilities should be appreciated from the perspectives IT, as well as non-IT. The assessment from both perspectives is critical, arising from insights obtained from the data analysis. In this regard, compliance systems tend to be managed or overseen by the Compliance department. Therefore, some of the capabilities being regarded as non-IT have the propensity to be utilised by this particular department, and further can be regarded as a source for attaining compliance benefits;

iv). Having fully appreciated the above, the assessment can continue to identify the associated supplementary benefits that could possibly arise from the realisation of compliance benefits. As has been revealed by the research, there was indeed a connection between appreciating and acknowledging compliance benefits with the identification of supplementary benefits [see Figure 7-1]. By significantly capitalising the appreciation of compliance benefits, the situation may facilitate the comprehensiveness in discovering possible supplementary benefits. Moreover, since the detected supplementary benefits have not arisen from the suggested deliberate efforts to incorporate optional considerations, they are instead regarded as being associated with possible alternative usage of compliance information. In this regard, compliance information that has been gathered; processed; and generated by regulatory IT systems may otherwise pose an opportunity to be used to directly benefit business;

v). Similarly, the assessment of supplementary benefits is also to be done in a structured and systematic manner, using the summary table as have been widely used in Chapter 7. Although the structured assessments is to be done using factors that are similar to the ones adopted for compliance benefits, one additional question need to be added in the attempt to ascertain the usefulness of the identified supplementary benefits. This additional assessment is included in order to importantly ascertain the practicality and feasibility of the identified benefits, as compared to other possible alternative sources that may produce similar and comparable benefits that have already existed within the organisation.
In relation to the assessment of associated capabilities, the identified capabilities for compliance benefits that can be linked to a particular supplementary benefits and used as a basis to further evaluate their influence in helping to attain the types of benefits that can positively influence organisation’s business; vi). Ultimately, further assessments need to be done in ascertaining how the utilisation of related capabilities in facilitating supplementary benefits have likely influence the organisation’s competitive positioning. In this regard, the assessment need to be done from the perspective of valuable; rarity; and appropriability attributes [see Section 3.4.3]. Importantly, the assessment will only be denoting the possibility of organisation achieving improved competitive positioning (ICP), and therefore, will not be indicating a clear competitive advantage has been achieved.

Moreover, the assessment on competitive positioning is also regarded as an important determinant in ascertaining whether any further system (and procedural) changes are worth pursuing. Complimentary investments (Davern and Kauffman, 2000) or further modifications, may be required in order to allow the identified supplementary benefits to be fully realised by the organisation, especially as part of an established organisational practice. In this regard, new information made available by the implementation of IT systems can also be considered as potentially guiding further organisational change (Doherty et al., 2012, Leonardi and Barley, 2010). This type of assessment can be used to provide the supporting justifications, if warranted, for obtaining subsequent management approval. Importantly, when it has been concluded that compliance system modifications to leverage expected business benefits will positively influence the organisation’s competitive positioning, the modifications process itself will eventually become purely mandatory or mainly mandatory investment activities (Joshi and Pant, 2008).

Viewing from a practical example arising from the data analysis, it is interesting to note that further modifications to Bank A’s IT systems may be warranted for a particular supplementary benefit to be realised in an efficient manner. In this regard, since the ISI; CBP; BK; and AIS capabilities have all exhibited the necessary
qualities to indicate ICP, therefore, related alterations to leverage AML/CFT false alerts should be deployed, since it has been regarded as a feasible and sensible effort [see Figure 8-6].

b) **Overall Justification for the Framework**

This framework provides a structured and systematic approach in determining the possibility, as well as the feasibility of leveraging business benefits from compliance systems. As the framework can be regarded as being independent of any particular type of compliance systems, it is envisaged that the implementation of the framework could be universally applied on any compliance system being deployed.

Literature regarding compliance systems and efforts to meet regulatory requirements has theoretically provided the notion of benefits that can be achieved in one form or another; such as through overall; broader; horizontal; unified; and process-based compliance approaches (e.g. Gable, 2005, Anderson, 2006, Garcia, 2004, Kulkarni, 2009). In addition, benefits are also said to be achievable through leveraging on certain functionalities or processes of the compliance systems e.g. utilising initial screening process for anti-money laundering to discover cross-selling opportunities (Anderson, 2006); or understanding customer to serve them better (Graham II, 2003, Garcia, 2004, Ruce, 2011).

Unfortunately, the suggestions in the literature can also be seen as piece meal approach as they tend to focus on a certain possible benefits suggested by the authors. Therefore, these suggestions do not in any way provide assurance that other possible benefits from a regulatory driven IT implementation have been thoroughly assessed and evaluated. Furthermore, the myriad compliance approaches and mechanisms suggested in the literature have primary inclination towards reducing compliance cost or increase compliance effectiveness (e.g. Garcia, 2004, Gable, 2005, Kulkarni, 2009). Hence, they do not provide any suggestions that the overall implementation of compliance systems, together with the expected actions and deliverables could be of any alternative usage or may possibly benefit organisation’s business directly.
Moreover, even though the work of Krell and Matook (2009) had recommended formal planning approach to be used in ensuring regulatory influenced IT systems modifications be aligned with business to achieve competitive advantage, it presents a less effective alternative to be utilised for systems that are purposely established for compliance. This is premised on the earlier understanding that evidence from data analysis, as well as the literature, has suggested that organisations would typically tend to rush to comply with regulatory requirements (Joshi and Pant, 2008). Therefore, they are less likely to include non-mandatory business requirements in mandatory system implementations.

Therefore, a framework to assess the possibility of leveraging potential benefits from compliance system implementations seemed to be significantly lacking in the literature. Equally important assessments to determine whether any systems (or procedural) changes are economically feasible and worth pursuing in order to achieve ICP, has likewise yet to be suggested by the literature. These considerations are over and above the unavailability of a common and structured assessment approach that could be universally implemented across all compliance systems being deployed within the organisation. Most importantly, the framework will present an opportunity for regulatory driven IT systems to counter the traditional thinking that views them as solely from the perspective of cost to the business.

Nevertheless, although possible benefits can be discovered by adopting the processes suggested by the framework, it is critical to note it does not in any way eliminate the potentiality of identifying possible benefits through the interactions between related departments. The discovery of potential benefits through departmental interactions has indeed been detected in the data analysis [see Section 8.2.5(a)]. In addition, it can also be supported by appreciating the suggestions provided in the literature (e.g. Anderson, 2006), i.e. particularly regarding compliance and marketing departments collaborations. The advantage of discussing with related parties may not only provide the opportunity to discover potential benefits, but could also be used to address practical issues such as addressing the possible confidentiality of some information generated by compliance systems.
Therefore, it is suggested that departmental interactions should be conducted especially when several important milestones have been achieved during the assessment process suggested by the framework. The key milestones in this regard, may include the point when the compliance and supplementary benefits need to assessed, as well as during the evaluation of competitive positioning that could subsequently be discovered.

9.4. **RESEARCH IMPLICATIONS**

As well as presenting a number of important new contributions to the literature, the study also provides a number of implications for practitioners working within the banking industry. The following section will discuss these implications in detail.

9.4.1. **Managerial Implications**

From the managerial perspective, an important consequence from the deployment of this research is pertaining to the specific knowledge on regulatory information that could alternatively be used by bankers to directly benefit business. In this regard, information that has been gathered, processed, and generated due to compliance may be used as one of the considerations to assess customers’ potential for an enhanced business relationship. As can be appreciated from the research findings, for example, genuine even-based customer information that is time-critical in nature, detected through AML/CFT monitoring, might indicate specific instances of a customer’s needs and wants. Similarly, IT repository containing cleansed customer transactions being gathered and processed for AML/CFT may likewise pose an opportunity to be leveraged by business for efficiency purposes.

More importantly, the practice of leveraging compliance information for business, in a structured and organised manner, may not only be limited to regulatory driven IT systems. This practice might also be extended by exploring similar possibilities with other systems for *business* that had to be urgently implemented, or as suggested by Krell et al. (2011: p. 633), to be in compliance with “*norms created by external*
organisations”. In this regard, this type of system may also be considered as mandatory as they have less flexibility of choice or timing, such as arising from the need to implement EDI or similar deployments mandated by major business partners (e.g. Joshi and Pant, 2008).

In addition to the above, a set of key capabilities that will assist in achieving regulatory expectations have also been identified by the study. These capabilities may be useful as a basis for organisations wishing to identify the critical competencies needed to achieve compliance. Moreover, these capabilities may also further facilitate the achievement of business benefits. Significantly, these capabilities can also be used as one of the conditions to decide whether changes to existing systems are worth pursuing, arising from their potential influence on organisation’s competitive positioning. Bank managers can therefore leverage these considerations during the effort to justify to the management, pertaining to the needed changes to leverage the identified business benefits.

Another important consequence for practitioners arising from the outcome of the research is, the revised framework to assess possible business benefits from regulatory IT implementations. Managers in banking institutions will be able to utilise the framework to universally conduct a systematic and structured assessment on all compliance systems being implemented by the organisation, or any systems for business that had to be urgently implemented.

9.5. PERSONAL REFLECTIONS

This study has provided great opportunity for the researcher to experience the learning process of conducting a ‘lone’ doctoral research project. While many issues were faced during the course of the project, this section will specifically highlight the challenges encountered during the two major data collection exercises, i.e. the first and the second phases. The reason to explicitly highlight these challenges can be attributed to their nature of being beyond the control of the researcher. Importantly, it is also to critically show that the position of the researcher being a central banker, had not in any way influenced any preferential treatment or smooth access to be
obtained from the research participants. Furthermore, it is also aimed to demonstrate that these commercial bankers were not seen as feeling somewhat obligated to participate in this study.

It is important to note at this juncture that although these challenges should not be likened to problems or difficulties that had significantly affected the study, it may worth noting their presence nevertheless, as they had somewhat influence the progression of the research.

As briefly mentioned in Section 4.5.3, some challenges were encountered during the effort to obtain appointments to interview the commercial bankers. Since the participation in the research is totally voluntary, not all requests to conduct interviews were successful, and the researcher did encounter several situations where the identified bankers had politely declined to participate.

Furthermore, there were also instances where several research participants had promised to provide contacts for identified colleagues or subordinates, as well as in a number of occasions, had assured that interviews will be arranged. However, in the end, these anticipated interviews were not conducted, as these bankers did not sincerely follow through their commitments, even though after repeated friendly reminders were made by the researcher.

Nevertheless, it is important to note that institutions that the researcher had experienced some challenges in dealing with, were random in nature and did not follow a specific pattern. The refusal to participate; non-responsiveness; or even non-committed promises, have no inclinations to be associated with any type of banking institutions, regardless of whether they are local or foreign-based organisations.

It needs to be noted that even though the above situations had occurred during the course of collecting research data, the research participants that the researcher had identified and wanted to interview within the two case study organisations, had been successfully conducted during the two main data collection exercises.

On a totally separate issue, the researcher had also encountered some challenges during the effort to transcribe the recorded interview conversations. In any research adopting the qualitative perspective, it is commonly accepted that transcription
process, as well as analysing interview transcripts are generally time consuming (e.g. Bryman, 2008, Ritchie, 2003). Nevertheless, it may be worth mentioning that the situation encountered by the researcher had unanticipatedly delayed the overall duration for transcription (and subsequently, analysis) of interview data. As mentioned in Section 4.5.2, interview conversations in this study were purposely recorded in a digital format, with the aim to allow the transcription process to be expedited using a reputable speech recognition software, known as Dragon NaturallySpeaking. Unfortunately, the software was totally unusable during transcription as it was not able to recognise the different English dialect commonly used by a typical Malaysian. Even though the researcher had tried to ‘train’ the software to recognise his voice in order to allow at least some part of the transcription process to be automated, the problem had still persisted.

9.6. LIMITATIONS OF THE STUDY

It is important to acknowledge the limitations this study, particularly on the applicability of the knowledge that it is trying to contribute. Generally, the empirical evidence generated by this study should only be regarded as being most appropriate in the context of banking institutions operating in Malaysia. Any attempt to generalise to a different possible settings such as for public listed companies within the securities market, or similar banking industry but within a totally different country, may need to be done with some caution. This is due to the different nature and characteristics of these settings, primarily in the form of totally different regulatory environment, as well as other possible contrasting factors, such as matters relating to social, political, and economic. These situations might significantly affect how the research is to be conducted and subsequently influence its associated research results.

Specifically, the limitation of this study can also be related to a possible bias, attributed to how the researcher had interpreted the situations that he had been exposed to during the conduct of the research (Doherty et al., 2012). Respondent bias can also arise in the form of interviewees stating what the researcher wants to hear (Bowen, 2005), although measures mitigating its occurrence have been taken [see
Section 4.6]. In addition, the study is also constrained by the understanding that the AML/CFT IT systems in Bank A and B were reviewed when they were at a contrasting stages of their life cycle, and thus any comparisons are to be made with extra care (Doherty et al., 2012). Moreover, the study’s limitation can also be associated with the relatively small number of case study organisations adopted by the research, as well as the number of interviews conducted within these case studies. Nevertheless, numerous interviews conducted in other organisations, including the regulatory authority, have been used to gain richer understanding, and assisted in contextualising the findings from the detailed case study organisations.

The final limitation of the study can relates to the lack of opportunity to practically test the feasibility of the revised framework. While it is acknowledged that the contributory factors that have led to its formulation were based on empirical evidence, it may further be helpful if the framework could be applied within a real life context. Testing of the framework was not done during the period when this research was conducted, mainly due to the inevitable time constraints of a doctoral research project (Mullins and Kiley, 2002).

9.7. OPPORTUNITIES FOR FUTURE RESEARCH

The overall motivation of this study is to highlight the potential IT value from a set of organisational systems that have been regarded as, thus far, not being given a sufficient amount of attention by researchers within the IS domain. Therefore, by being one of the few studies that has genuinely attempted to investigate this particular area of interest, more work may need to be done. This is particularly in terms of further possible evaluation; replication; re-examination and possibly extension, employing different methods and in potentially different contexts.

Specifically, by reemphasising the statements made in the preceding section, the revised framework suggested by this study is in the need of being assessed from the perspective of real life deployment. Therefore, it would be useful if future research can make an effort to test the revised framework. Besides confirming on its suitability,
this effort could possibly lead to its further refinement, based on any practical challenges that may arise.

The review of the framework in action may possibly be done from the context of two contrasting organisations. Firstly, the framework could be tested on organisations that may likely to appreciate the notion of leveraging regulatory IT implementations to directly benefit business. This particular approach is selected in order to confirm the feasibility and practicality of the framework, which may also lead to its further enhancements. Meanwhile, the second type of organisations could be the ones having contrasting level of receptiveness, in order to ascertain the reasons and situations where the framework would be considered as unsuitable.

In addition to the above, it would likewise be useful if the framework can be tested using a different type of regulatory driven IT systems, that may have similar potential of bringing supplementary benefits to the organisation. Furthermore, it may likewise be interesting if the testing could also be extended to other systems for business that had to be urgently implemented, which can also be considered as mandatory systems possessing less flexibility of choice or timing.

9.8. CONCLUDING REMARKS

This chapter provides summarisation for the whole thesis through the presenting the overall findings and comparing with the research objectives; implications; and importantly a revised framework that is thought to be better suited for ascertaining possible benefits of regulatory driven IT implementations. With all the research objectives have indeed been addressed, further gaps identified, and a revised framework is suggested, it can therefore be regarded that this study has made several valuable contribution to the body of literature relating to this area of interest.
List of References


GLASER, B. & STRAUSS, A. 1967. The Discovery of Grounded Theory, Aldine, Chicago, IL.


List of References


List of Appendices

Appendix I: Sample Questions in the Interview Guide .................................................... 329
Appendix II: Sample Email to Banking Institutions ......................................................... 330
Appendix III: Letter from the University ........................................................................ 331
Appendix IV: Letter from the Central Bank of Malaysia .................................................... 332
Appendix V: The Participation Information Sheet ............................................................. 333
Appendix VI: The Informed Consent Form ...................................................................... 337
Appendix VII: Key Document Sources ......................................................................... 338
Appendix VIII: Required Changes/Actions Motivated by AML/CFT Requirements .... 339
Appendix IX: Additional Sections Necessitating Effective CDD Process ................. 370
Appendix X: Requirements to Obtain and Maintain Customer Information .................. 372
Appendix XI: Overview on Analysis of Capabilities ......................................................... 375
Appendix I: Sample Questions in the Interview Guide

1. Could you give an example of a key IT system that has been successfully implemented in your organisation?

2. Could you name the regulations that have an important influence on the key IT system that you have just mentioned? In what way they have shaped and influence this IT system?

3. Can you explain the processes involved in ensuring this key IT system is complying with the requirements of the regulations that you have just mentioned?

4. What are the skills required when complying with regulations?

5. How do you justify the required investment to your management?

6. Do you detect any similarities or overlapping requirements with other regulations? If yes, please explain how you handle those similarities?

7. Do you take into account any other considerations or information (e.g. threats, opportunities) beyond what were required?

8. Are there any positive aspects that you discovered arising from complying with these regulations?

9. In your opinion, what are the potential benefits in complying with these guidelines?

10. What are the skills required to experience these benefits (if any)?

11. Do you think the similar benefit can be leveraged by other banks (if any)? What causes this benefit to be unique to your bank?

12. When discover exceptions, explore the following:
   - Explain in detail how information from compliance system is being used for business purposes?
   - Where did the idea came from? What causes it to occur?
   - Why and how is it unusual (determine how do they reach this level of receptiveness)?
   - What is your view on Compliance and its role / how does Compliance see themselves?
   - Are there any historical reasons behind it?
   - Why this is allowed?
Appendix II: Sample Email to Banking Institutions

Dear <name>,

As mentioned during our phone conversation on <date>, I attached herewith the related documents that provide some background on my research, as well as, letters from Loughborough University and Bank Negara Malaysia.

I am seeking to interview <organisation’s name> member of staff who has any experience relating to compliance activities, particularly involving changes to any of <organisation’s name>’s IT systems. If possible, I will be very grateful if I am able to speak to at least someone from Compliance, IT and Business/Operations, if possible.

Please feel free to contact me if further clarifications are needed. I can also liaise directly with the members of staff that are willing to be interviewed, if you are able to provide me their contact details (name, phone numbers and email addresses).

Many thanks for your kind assistance.

Best wishes,
Abdullah

Abdullah Othman
Doctorate Researcher
The Business School
Loughborough University
LE11 3TU, United Kingdom
Email: A.Othman@lboro.ac.uk
Phone: +44 (0)1509 223239
Appendix III: Letter from the University

Business School
Loughborough University  Leicestershire  LE11 3TU  UK
Switchboard: +44 (0)1509 263171  www.lboro.ac.uk/businessschool

To whom it may concern

17th May 2010

Dear Sir/Madam

Re – Mr Abdullah Othman

This letter is to confirm that Abdullah Othman, Student ID No A819623, is a Doctoral Researcher at The Business School, Loughborough University. His research is focusing upon the impact of regulations upon the value of IT investments, within Malaysian banking institutions. As part of the requirement for his research, he will be conducting face to face interviews with selected members of staff, within Malaysian banking institutions. I would therefore be extremely grateful if you could provide him with the necessary cooperation and access he needs, in order to ensure that his research studies can be effectively undertaken.

If you require further information or clarifications, please refer the ‘Participant Information Sheet’ and ‘Informed Consent Form’, or alternatively, please feel free to contact me directly.

Yours faithfully

[Signature]

N.F. Doherty
Professor of Information Management
Appendix IV: Letter from the Central Bank of Malaysia

13 May 2010

To Whom It May Concern,

Dear Sir,

This is to confirm that Mr. Abdullah bin Othman is a staff and scholar of Bank Negara Malaysia. He is currently pursuing PhD in Loughborough University, United Kingdom.

Yours sincerely,

(RAFIDAH LATIF)
For Director
Appendix V

Appendix V: The Participation Information Sheet

Loughborough University

Participant Information Sheet

Researchers’ Contact Details

Main Investigator / Researcher:
Abdullah Othman, Doctoral Researcher
The Business School, Loughborough University, Loughborough, Leicestershire, LE11 3TU, UK.
Email: A.Othman@lboro.ac.uk
Phone: +44 (0)1509 223239

Research Supervisors:
Professor Neil F. Doherty, Professor of Information Management
The Business School, Loughborough University, Loughborough, Leicestershire, LE11 3TU, UK.
Email: N.F.Doherty@lboro.ac.uk
Phone: +44 (0)1509 223128

Dr Amany Elbanna, Lecturer in Information Systems
The Business School, Loughborough University, Loughborough, Leicestershire, LE11 3TU, UK.
Email: A.Elbanna@lboro.ac.uk
Phone: +44 (0)1509 222435

What is the purpose of the study?
This research aims to gain understanding on how the process of regulatory compliance, that has an impact on IT systems, is being carried out by banking institutions in Malaysia. It seeks to gain insights on the compliance approach adopted, focusing upon, among others, the activities involved; the required resources; skills and information needed to facilitate compliance of banking IT systems to regulations...
Appendix V

issued by the regulatory authorities. In addition, this study aims to understand and appreciate any good practices employed by banking institutions with regard to their compliance activities. Finally, it aims to comprehend how the value of banking IT investments have been affected or influenced by the compliance related activities and the results of being compliant.

Who is doing this research and why?

This research is conducted by Abdullah Othman, a Doctoral Researcher at The Business School, Loughborough University. His doctorate research is being monitored and supervised by two academic staff at the School, i.e. Professor Neil F. Doherty and Dr Amany Elbanna.

Abdullah’s doctorate study is sponsored by Bank Negara Malaysia (i.e. the Central Bank of Malaysia), which Abdullah is also an employee but currently on study leave. However, it is worth noting that even though Abdullah is being sponsored by the central bank, he is under no obligation to report the results of his study to his sponsor. More importantly, Abdullah has to adhere to the strict requirements prescribed by the University with regard to confidentiality and non-identifiably of information gathered throughout his research. Furthermore, the interview will be guided by an interview guide which defines the areas that Abdullah will be covering. This interview guide has been endorsed by the research supervisors and has adhered to the requirements imposed by the University.

Once I take part, can I change my mind?

Absolutely. After you have read this information and asked any questions you may have, we will ask you to complete an Informed Consent Form, however if at any time, before, during or after the sessions you wish to withdraw from the study please just contact the main investigator / researcher or his supervisors. You can withdraw and require your data to be destroyed at any time, for any reason and you will not be asked to explain your reasons for withdrawing.

Will I be required to attend any sessions and where will these be?

If you agree to being interviewed, the interview will take place in a convenient location that allows for the protection of your privacy and confidentiality.
Appendix V

How long will the interview take?
The interview session is expected to last for approximately one hour depending on the situation.

Is there anything I need to do before the sessions?
You will be asked to sign an Informed Consent Form.

What personal information will be required from me?
We would appreciate your contact details (name, phone number and email address) for us to contact you if we need to seek further clarifications.

Are there any risks in participating?
We are of the view that this research poses no risk to you. Generally, we seek to understand how your organisation typically performed its compliance activities in the past and we do acknowledge that there is no right or wrong approach to compliance. All information will be treated as highly confidential, and results of the research will only be reported in an aggregate or non-identifiable manner. In addition, you do not have to answer any questions you do not want to, and you will not be asked to explain your reasons for declining to answer a question.

Will my taking part in this study be kept confidential?
Definitely. As mentioned in a prior section, all information gathered throughout this research will be securely kept and treated as highly confidential, else it will adversely affect the credibility of the researchers and their research outputs.

The recorded interview will be transcribed and subsequently analysed to detect common themes. All information gathered in this research will only be made available to researcher, as well as, his research supervisors for monitoring and analysis purposes. No raw data will (or can) be shared or published to third parties. Details of interviewees and the transcribed interview data will be kept separately (e.g. interviewees will be identified as Interviewee 1, 2 and so on, and pseudonyms will be used in the transcribed interview document and citing of quotations). All interview files and documents are therefore anonymous and non-identifiable.
Furthermore, under the University guidelines:

- Any numerical/statistical data will be stored in raw data format only for the length of time necessary for the research (and not for no more than six years from completion of the project) and will be destroyed afterwards;
- Any interview notes and recorded and transcribed interviews will be stored in their original form only for the length of time necessary for the research (and for no more than ten years from completion of the project) and will be destroyed afterwards; and
- Any processing of personal data will comply with the requirements of UK’s Data Protection Act 1998.

What will happen to the results of the study?

The results of the study will be written up for publication as a PhD thesis, may be presented in an academic conference and may be published in an academic/professional articles and/or book. The results will be written and reported in an aggregate or non-identifiable manner. Ownership of the data and all writing relating to the research will reside with the researchers.

I have some more questions who should I contact?

You can contact the research supervisors through their contact details stated on the first page of this document.

What if I am not happy with how the research was conducted?

You can contact the research supervisors through their contact details stated on the first page of this document. In addition, the University has a policy relating to Research Misconduct and Whistle Blowing which you can access online at: [http://www.lboro.ac.uk/admin/committees/ethical/Whistleblowing(2).htm](http://www.lboro.ac.uk/admin/committees/ethical/Whistleblowing(2).htm).
Appendix VI: The Informed Consent Form

INFORMED CONSENT FORM
(to be completed after Participant Information Sheet has been read)

The purpose and details of this study have been explained to me. I understand that this study is designed to further scientific knowledge and that all procedures have been approved by the Loughborough University Ethical Advisory Committee.

I have read and understood the information sheet and this consent form.

I have had an opportunity to ask questions about my participation.

I understand that I am under no obligation to take part in the study.

I understand that I have the right to withdraw from this study at any stage for any reason, and that I will not be required to explain my reasons for withdrawing.

I understand that all the information I provide will be treated in strict confidence and will be kept anonymous and confidential to the researchers unless (under the statutory obligations of the agencies which the researchers are working with), it is judged that confidentiality will have to be breached for the safety of the participant or others.

I agree to participate in this study.

Your name

______________________________

Your signature

______________________________

Signature of investigator

______________________________

Date

______________________________
## Appendix VII: Key Document Sources

<table>
<thead>
<tr>
<th>Organisation</th>
<th>Name of Document</th>
<th>Document No</th>
</tr>
</thead>
<tbody>
<tr>
<td>The United Nations; and other international bodies</td>
<td>United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988)</td>
<td>D001</td>
</tr>
<tr>
<td></td>
<td>Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (1990)</td>
<td>D004</td>
</tr>
<tr>
<td></td>
<td>Inter-American Convention Against Terrorism (2002)</td>
<td>D005</td>
</tr>
<tr>
<td></td>
<td>FATF IX Special Recommendations (2001)</td>
<td>D007</td>
</tr>
<tr>
<td></td>
<td>Customer Due Diligence for Banks (2001)</td>
<td>D009</td>
</tr>
<tr>
<td>Bank A</td>
<td>AML/CFT system briefing slides</td>
<td>D014</td>
</tr>
<tr>
<td></td>
<td>RSA2 system KYC presentation slides</td>
<td>D015</td>
</tr>
<tr>
<td></td>
<td>Opening of Account Forms</td>
<td>D016</td>
</tr>
<tr>
<td></td>
<td>International Conference on Financial Crime and Terrorism Financing (ICFCTF) 2010 presentation slides</td>
<td>D017</td>
</tr>
<tr>
<td></td>
<td>CRM Excellence Award Submission Report 2010</td>
<td>D018</td>
</tr>
<tr>
<td></td>
<td>CRM1 system’s logical architecture (Phase 3 Release 1 &amp; 2)</td>
<td>D019</td>
</tr>
<tr>
<td>Bank B</td>
<td>Risk Profiling in RSB1 System</td>
<td>D020</td>
</tr>
</tbody>
</table>
## Appendix VIII: Required Changes/Actions Motivated by AML/CFT Requirements

<table>
<thead>
<tr>
<th>No</th>
<th>Required Changes / Actions</th>
<th>Related Sections</th>
<th>Expected Deliverables</th>
<th>Compliance Benefits</th>
<th>Supplementary Benefits</th>
</tr>
</thead>
</table>
| 1. | Develop customer acceptance policies and procedures to cater for the commencement of business relationship with the customer. | STG, 4.1.1       | • Establishment of or enhancement to manual policies and procedures on customer acceptance.  
• Establishment of or enhancement to customer acceptance module in the business IT system.                                                                 | • Ability to effectively monitor and detect activities pertaining to ML/TF.  
• Ability to mitigate the risk of financial or non-financial penalties due to non-compliance imposed by the regulatory authority (cost avoidance).(042; 041; 004; 008)  
• Ability to mitigate the risk of adverse implications to the image of the organisation (i.e. reputational risk) due to being associated with ML/TF.(039; 006; 003; 034; 008)  
• Ability to facilitate overseas banking operations (e.g. establishing overseas branches or providing corresponding banking services) by meeting the requirements on AML/CFT.(016) | • Opportunity to select desired and reject undesired new customers through AML/CFT screening process during opening of new banking accounts or establishing new banking relationships.(039; 042; 006; 003; 019) |
| 2. | Conduct risk profiling to identify and assess the risk of the customers, and implement reasonable measures to address different customers’ risks. | STG, 4.1.1 & 4.1.2 | • Establishment of or enhancement to manual policies and procedures on customer risk profiling and addressing different customers’ risks.  
• Establishment of or enhancement to customer risk                                                                 | • Ability to effectively monitor and detect activities pertaining to ML/TF.  
• Ability to mitigate the risk of financial or non-financial penalties due to non-compliance imposed by the regulatory authority (cost avoidance).(042; 041; 004; 008) | • Opportunity to segment customers according to their risk categorisations.  
• Opportunity to identify customers that are of low and medium risks which could be targeted for business relationship enhancements (e.g. |
<table>
<thead>
<tr>
<th>No</th>
<th>Required Changes / Actions</th>
<th>Related Sections</th>
<th>Expected Deliverables</th>
<th>Compliance Benefits</th>
<th>Supplementary Benefits</th>
</tr>
</thead>
</table>
|    |                            |                 | profiling module in the AML/CFT IT system.  
• Availability of customers’ information that has been risk categorised e.g. low, medium, and high risk customers. | Ability to mitigate the risk of adverse implications to the image of the organisation (i.e. reputational risk) due to being associated with ML/TF.(039; 006; 003; 034; 008)  
• Ability to facilitate overseas banking operations (e.g. establishing overseas branches or providing corresponding banking services) by meeting the requirements on AML/CFT.(016)  
• Ability to implement a monitoring process that is emphasised on customers’ risk categorisations.  
• Ability to identify customers that of higher risk or tendency to be associated with ML/TF.  
• Ability to deploy enhanced precautionary measures when dealing with customers that are considered risky from the perspective of AML/CFT (003). | cross-selling, differential pricing and promotional campaigns, etc.) at a later period or when the need arises. |
| 3. | Conduct risk profiling that consider (at minimum) information such as:  
• The customer’s origin and business location;  
• The customer’s background or profile;  
• The customer’s nature of | STG, 4.2.1 | Establishment of or enhancement to manual policies and procedures on customer risk profiling.  
Establishment of or enhancement to customer risk profiling module in the AML/CFT IT system. | Ability to effectively monitor and detect activities pertaining to ML/TF.  
Ability to mitigate the risk of financial or non-financial penalties due to non-compliance imposed by the regulatory authority (cost avoidance).(042; 041; 004; 008) | Opportunity to segment customers according to their risk categorisations.  
Opportunity to correctly pinpoint customers (based on the information obtained) that are of low and medium risks which could be targeted for business |
<table>
<thead>
<tr>
<th>No</th>
<th>Required Changes / Actions</th>
<th>Related Sections</th>
<th>Expected Deliverables</th>
<th>Compliance Benefits</th>
<th>Supplementary Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>business; • The customer’s structure of ownership (i.e. for corporate customer); and • Other information that may indicate that the customer is of higher risk.</td>
<td></td>
<td>• Availability of customers’ information that has been risk categorised e.g. low, medium, and high risk customers, and information that has been grouped according to background, origin, nature and location of business, etc.</td>
<td>• Ability to mitigate the risk of adverse implications to the image of the organisation (i.e. reputational risk) due to being associated with ML/TF.(039; 006; 003; 034; 008) • Ability to facilitate overseas banking operations (e.g. establishing overseas branches or providing corresponding banking services) by meeting the requirements on AML/CFT.(016) • Ability to implement monitoring process that is emphasised on customers’ risk categorisations and classifications. • Ability to identify customers that of higher risk or tendency to be associated with ML/TF. • Ability to implement enhanced precautionary measures in business relationship with customers that are considered risky from the perspective of AML/CFT (003).</td>
<td>relationship enhancements (e.g. cross-selling, differential pricing and promotional campaigns, etc.) at a later period or when the need arises. • Opportunity to guide organisation’s future business relationship enhancement efforts based on information such as customer’s background, origin, as well as nature and location of business, etc. (for example; focusing possible marketing efforts on customers of medium risk located in a favourable location).</td>
</tr>
<tr>
<td>4.</td>
<td>Ensure consistency of customer’s risk profile by continuously monitor customer’s transaction activity pattern. Unreasonable difference should prompt</td>
<td>STG, 4.2.2</td>
<td>• Establishment of or enhancement to manual policies and procedures on monitoring of customers’ transactional activities against their risk profiles.</td>
<td>• Ability to effectively monitor and detect activities pertaining to ML/TF. • Ability to mitigate the risk of financial or non-financial penalties due to non-compliance imposed</td>
<td>• Opportunity to access accurate and up-to-date customer’s risk profile information that could be used for business relationship enhancement activities (e.g. cross-selling, differential pricing,</td>
</tr>
<tr>
<td>No</td>
<td>Required Changes / Actions</td>
<td>Related Sections</td>
<td>Expected Deliverables</td>
<td>Compliance Benefits</td>
<td>Supplementary Benefits</td>
</tr>
<tr>
<td>----</td>
<td>----------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>4.</td>
<td>reassessment of customer risk profile.</td>
<td></td>
<td>* Establishment of or enhancement to customer risk profiling and monitoring module in the AML/CFT IT system. Key AML/CFT IT system functionalities that would assist in meeting this requirement are:</td>
<td>* Ability to mitigate the risk of adverse implications to the image of the organisation (i.e. reputational risk) due to being associated with ML/TF.(039; 006; 003; 034; 008) * Ability to facilitate overseas banking operations (e.g. establishing overseas branches or providing corresponding banking services) by meeting the requirements on AML/CFT.(016) * Ability to ensure the integrity and currency of customers’ risk profiling information, which would facilitate accurate identification of a customer that has been suspected to be associated with ML/TF.</td>
<td>* Opportunity to increase the productivity and effectiveness of organisation’s business relationship enhancement efforts (e.g. cross selling, marketing, etc.) by having access to accurate and up-to-date information.</td>
</tr>
<tr>
<td>5.</td>
<td>Regularly review and update customers’ risk profiles, particularly due to changes in employment or nature of business.</td>
<td>SCG1, 3.1.1</td>
<td>* Establishment of or enhancement to manual policies and procedures on periodic review on and update of customers’ risk profiles. * Establishment of or enhancement to customer risk profiling module in the AML/CFT IT system to include periodic review of customer risk profiles.</td>
<td>* Ability to effectively monitor and detect activities pertaining to ML/TF. * Ability to mitigate the risk of financial or non-financial penalties due to non-compliance imposed by the regulatory authority (cost avoidance).(042; 041; 004; 008) * Ability to mitigate the risk of adverse implications to the image.</td>
<td>* Opportunity to access accurate and up-to-date customer’s risk profile information, particularly due to changes in employment (017) and nature of business, which could be used for business relationship enhancement activities (e.g. cross-selling, differential pricing and promotional campaigns, etc.) at a later period or when the need arises.</td>
</tr>
<tr>
<td>No</td>
<td>Required Changes / Actions</td>
<td>Related Sections</td>
<td>Expected Deliverables</td>
<td>Compliance Benefits</td>
<td>Supplementary Benefits</td>
</tr>
<tr>
<td>----</td>
<td>-----------------------------</td>
<td>------------------</td>
<td>-----------------------</td>
<td>---------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Key AML/CFT IT system functionalities that would assist in meeting this requirement are: • customer due diligence, • behaviour profiling, • suspicious transactions monitoring, • alert management, and • link analysis. • Availability of exception reports based on the requirement (i.e. report on changes to customers' risk profiles due to changes in employment or nature of business).</td>
<td>of the organisation (i.e. reputational risk) due to being associated with ML/TF. (039; 006; 003; 034; 008) • Ability to facilitate overseas banking operations (e.g. establishing overseas branches or providing corresponding banking services) by meeting the requirements on AML/CFT. (016) • Ability to ensure the integrity and currency of customers' risk profiling information (i.e. arising from changes in employment (017) and nature of business), that facilitates accurate identification of a customer that has been suspected to be associated with ML/TF. • Ability to effectively monitor and detect activities pertaining to ML/TF. • Ability to mitigate the risk of financial or non-financial penalties due to non-compliance imposed by the regulatory authority (cost avoidance). (042; 041; 004; 008) • Ability to mitigate the risk of adverse implications to the image of the organisation (i.e. reputational risk) due to being later period or when the need arises. • Opportunity to increase the productivity and effectiveness of organisation's business relationship enhancement efforts (e.g. cross selling, marketing, etc.) by having access to accurate and up-to-date information.</td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>Ensure that accounts are maintained in the account holder’s name, and not anonymous; fictitious; false or incorrect.</td>
<td>AMLATFA, sections 16(1)(a) and (b), and section 18(1)</td>
<td>• Establishment of or enhancement to manual policies and procedures on maintaining customer details. • Establishment of or enhancement to the controls implemented to capture and validate customer details in the business IT system. • Availability of accurate and validated information on name of customers.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Appendix VIII
### Customer Due Diligence

<table>
<thead>
<tr>
<th>No</th>
<th>Required Changes / Actions</th>
<th>Related Sections</th>
<th>Expected Deliverables</th>
<th>Compliance Benefits</th>
<th>Supplementary Benefits</th>
</tr>
</thead>
</table>
|    | Perform CDD when customer wish to commence a business relationship with the bank:  
  - Obtain adequate proof and accurately establish the individual’s identity and legal existence.  
  - All evidences must be confirmed by reliable and independent source documents. | STG, 5.1.1; AMLATFA, sections 16(2)(a) and (b) |  
  - Establishment of or enhancement to manual policies and procedures on due diligence for engaging with new customers.  
  - Establishment of or enhancement to CDD process for new customers in the business IT system.  
  - Availability of accurate and validated customers’ information. |  
  - Ability to effectively monitor and detect activities pertaining to ML/TF.  
  - Ability to mitigate the risk of financial or non-financial penalties due to non-compliance imposed by the regulatory authority (cost avoidance).  
  - Ability to mitigate the risk of adverse implications to the image of the organisation (i.e. reputational risk) due to being associated with ML/TF. |  
  - Opportunity to access accurate and validated customer’s information that could be used to correctly pinpoint targeted customers for business relationship enhancement activities (e.g. cross-selling, differential pricing and promotional campaigns, etc.) at a later period or when the need arises.  
  - Opportunity to increase the productivity and effectiveness of organisation’s business relationship enhancement efforts (e.g. cross selling, marketing, etc.) by having access to accurate and validated information on customers. |
### Appendix VIII

<table>
<thead>
<tr>
<th>No</th>
<th>Required Changes / Actions</th>
<th>Related Sections</th>
<th>Expected Deliverables</th>
<th>Compliance Benefits</th>
<th>Supplementary Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.</td>
<td>Perform CDD when:</td>
<td>STG, 5.1.2;</td>
<td>• Establishment of or</td>
<td>providing corresponding banking services by meeting the requirements on AML/CFT. (016)</td>
<td>and validated information.</td>
</tr>
<tr>
<td></td>
<td>- A transaction has exceeded the amount specified by the regulatory authority under the SCG1 or relevant circular. CDD need to be conducted when transactions are:</td>
<td>SCG1, 4.1.2 to 4.1.6</td>
<td>enhancement to manual policies and procedures on CDD for the required category and type of transactions, as well as transactions that are considered as suspicious.</td>
<td>• Ability to ensure that customers are adequately and accurately identified and validated.</td>
<td>• Opportunity to reject undesired new customers through AML/CFT screening process during opening of new banking account or establishing new banking relationship. (039; 042; 006; 003; 019).</td>
</tr>
<tr>
<td></td>
<td>- RM20,000 and above for Bureau de Change services;</td>
<td></td>
<td>• Establishment of or enhancement to CDD process in the business IT system to cater for the required category and type of transactions, as well as transactions that are considered as suspicious.</td>
<td>• Ability to effectively monitor and detect activities pertaining to ML/TF.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- RM50,000 and above for occasional or cash transactions. For cash transactions of this category, CDD must be conducted on the customer, as well as the person conducting the transaction; and</td>
<td></td>
<td>• Availability of exception reports based on the requirement (i.e. report on transactions that have reached or exceeded the specified thresholds for the required category and type of transactions, as well as for suspicious transactions).</td>
<td>• Ability to mitigate the risk of financial or non-financial penalties due to non-compliance imposed by the regulatory authority (cost avoidance). (042; 041; 004; 008)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- RM3,000 and above for wire transfers. For this type of transactions,</td>
<td></td>
<td></td>
<td>• Ability to mitigate the risk of adverse implications to the image of the organisation (i.e. reputational risk) due to being associated with ML/TF. (039; 006; 003; 034; 008)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Ability to facilitate overseas banking operations (e.g. establishing overseas branches or providing corresponding banking services) by meeting the requirements on AML/CFT. (016)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Ability to detect and comprehend customers’ financial transaction anomalies through the</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Opportunity to detect genuine customer’s transactions (i.e. false alerts) that could be used to trigger, as well as be an input to time-critical event-based business relationship enhancement activities (e.g. cross-selling, differential pricing and promotional campaigns, etc.) of the organisation.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Opportunity to increase the productivity and effectiveness of organisation’s business relationship enhancement efforts (i.e. increase the chances of achieving success) by having the ability to detect time-critical event-based customers’ information, discovered through the due diligence process established for AML/CFT.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Opportunity to mitigate the risk of inadvertently prospecting</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>Required Changes / Actions</td>
<td>Related Sections</td>
<td>Expected Deliverables</td>
<td>Compliance Benefits</td>
<td>Supplementary Benefits</td>
</tr>
<tr>
<td>----</td>
<td>-----------------------------</td>
<td>------------------</td>
<td>-----------------------</td>
<td>---------------------</td>
<td>------------------------</td>
</tr>
</tbody>
</table>
| 9  | accurate and meaningful originator information is required to be transmitted.  
   • Regardless of the amount transacted, if:  
     • The reporting institution has any reason to suspect the legitimacy of the transaction. CDD must be conducted on the customer, as well as the person conducting the transaction;  
     • The reporting institution has any doubt about the accuracy or adequacy of information obtained previously; and  
     • The reporting institution has any suspicion of ML/TF. | STG, 5.1.3 & 5.6.1; AMLATFA, sections 16(2)(a) and (b), section 16(3) | • Establishment of or enhancement to manual policies and procedures on CDD to capture and verify the required information.  
• Establishment of or enhancement to CDD process in the business IT system to capture and verify the required information. | • Ability to effectively monitor and detect activities pertaining to ML/TF.  
• Ability to mitigate the risk of financial or non-financial penalties due to non-compliance imposed by the regulatory authority (cost avoidance).(042; 041; 004; 008)  
• Ability to mitigate the risk of customers that may turn out to be associated with ML/TF (as the triggering customers’ information is detected from transactions that have been deemed as genuine). | • Opportunity to access accurate and up-to-date customer’s information that could be used to correctly pinpoint targeted customers for business relationship enhancement activities (e.g. cross-selling, differential pricing and promotional campaigns, etc.) at a |
<table>
<thead>
<tr>
<th>No</th>
<th>Required Changes / Actions</th>
<th>Related Sections</th>
<th>Expected Deliverables</th>
<th>Compliance Benefits</th>
<th>Supplementary Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>transaction, if there is any suspicion that the transaction is conducted on behalf of a beneficial owner;</td>
<td>SCG1, 4.1.1</td>
<td>information.</td>
<td>adverse implications to the image of the organisation (i.e. reputational risk) due to being associated with ML/TF.(039; 006; 003; 034; 008)</td>
<td>later period or when the need arises.</td>
</tr>
<tr>
<td></td>
<td>• Determine the purpose and intention of the business relationship or transaction; and</td>
<td></td>
<td>• Availability of accurate and validated customers’ information.</td>
<td>• Ability to facilitate overseas banking operations (e.g. establishing overseas branches or providing corresponding banking services) by meeting the requirements on AML/CFT.(016)</td>
<td>• Opportunity to increase the productivity and effectiveness of organisation’s business relationship enhancement efforts by having access to accurate and up-to-date information on customers.</td>
</tr>
<tr>
<td></td>
<td>• Ensure information provided is continuously updated and relevant.</td>
<td></td>
<td></td>
<td>• Ability to ensure that customers’ information is adequately and accurately identified and updated, which ensures its integrity and currency.</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>The extent of customers’ information required during identification stage would depends on:</td>
<td></td>
<td>• Establishment of or enhancement to manual policies and procedures on CDD to incorporate the extent of customer information needed from selected customers during identification stage.</td>
<td>• Ability to effectively monitor and detect activities pertaining to ML/TF.</td>
<td>• Opportunity to access additional and extra information from selected customers that could be used for business relationship enhancement activities (e.g. cross-selling, differential pricing and promotional campaigns, etc.) at a later period or when the need arises.</td>
</tr>
<tr>
<td></td>
<td>• The risk of ML/TF based on the customer background and the situation pertaining to the transaction that could be seen as suspicious;</td>
<td></td>
<td>• Establishment of or enhancement to CDD process in the business IT system to incorporate the extent of customer information needed from selected customers during identification stage.</td>
<td>• Ability to mitigate the risk of financial or non-financial penalties due to non-compliance imposed by the regulatory authority (cost avoidance).(042; 041; 004; 008)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The type or form of transaction, and whether it involves a new product or service, or utilising new technology; and</td>
<td></td>
<td></td>
<td>• Ability to mitigate the risk of adverse implications to the image of the organisation (i.e. reputational risk) due to being associated with ML/TF.(039; 006; 003; 034; 008)</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>Required Changes / Actions</td>
<td>Related Sections</td>
<td>Expected Deliverables</td>
<td>Compliance Benefits</td>
<td>Supplementary Benefits</td>
</tr>
<tr>
<td>----</td>
<td>--------------------------------------------------------------------------------------------</td>
<td>----------------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>• The customer’s type (either account holders or non-account holders) and which entities they represent.</td>
<td></td>
<td>• Availability of additional and extra information from selected customers.</td>
<td>• Ability to facilitate overseas banking operations (e.g. establishing overseas branches or providing corresponding banking services) by meeting the requirements on AML/CFT.(016)</td>
<td>and extra information from selected customers.</td>
</tr>
<tr>
<td></td>
<td>11 Terminate business relationship (with existing customers) or prevent from commencing business relationship (with new customers) that failed to comply with the CDD requirements.</td>
<td>STG, 5.1.5</td>
<td>• Establishment of or enhancement to manual policies and procedures on CDD to incorporate the actions to be taken on customers that failed to meet the due diligence requirements.</td>
<td>• Ability to effectively monitor and detect activities pertaining to ML/TF.</td>
<td>• Opportunity to select desired and reject undesired new customers through AML/CFT due diligence process during opening of new banking account or establishing new banking relationship.(039; 042; 006; 003; 019)</td>
</tr>
<tr>
<td></td>
<td>• Establishment of or enhancement to CDD process in the business IT system and AML/CFT IT system to incorporate the actions to be taken on customers that failed to meet the CDD requirements. Key AML/CFT IT system functionality</td>
<td></td>
<td>• Ability to mitigate the risk of financial or non-financial penalties due to non-compliance imposed by the regulatory authority (cost avoidance).(042; 041; 004; 008)</td>
<td>• Ability to mitigate the risk of adverse implications to the image of the organisation (i.e. reputational risk) due to being associated with ML/TF.(039; 006; 003; 034; 008)</td>
<td>• Opportunity to terminate undesired existing customer relationships that failed to meet the organisation’s due diligence process.(039; 042; 006; 003; 019)</td>
</tr>
<tr>
<td></td>
<td>• Ability to facilitate overseas banking operations (e.g. establishing overseas branches or providing corresponding banking services) by meeting the requirements on AML/CFT.(016)</td>
<td></td>
<td>• Ability to ensure that additional and extra information from selected customers is adequately and accurately obtained for the purpose of identification.</td>
<td>• Opportunity to focus the organisation’s effort to enhance business relationship with valued customers.</td>
<td></td>
</tr>
</tbody>
</table>

1 Where the AML/CFT risk is low and verification is not possible when establishing business relationship, the customer due diligence process can be completed within 14 days, to permit the customer to furnish the required documentary evidence. The risk of delayed validation is to be mitigated by establishing appropriate policies and procedures (such as limiting the number and type of transactions that the customer can perform).
<table>
<thead>
<tr>
<th>No</th>
<th>Required Changes / Actions</th>
<th>Related Sections</th>
<th>Expected Deliverables</th>
<th>Compliance Benefits</th>
<th>Supplementary Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>that would assist in meeting this requirement:</td>
<td>establishing overseas branches or providing corresponding banking services) by meeting the requirements on AML/CFT.(016) • Ability to effectively and efficiently address customers that failed to meet the organisation’s CDD requirements.</td>
<td>(i.e. residual) customers that have been retained once relationships with undesired customers (and suspected money launderers) are ceased.(042)</td>
</tr>
<tr>
<td>12</td>
<td>CDD on an individual customer should (at minimum) require:</td>
<td>STG, 5.2.1 &amp; 5.2.3; SCG1, 4.2.1</td>
<td>• Establishment of or enhancement to manual policies and procedures on CDD for individual customers to obtain and verify the required information. • Establishment of or enhancement to CDD process in the business IT system for individual customers to obtain and verify the required information. • Availability of accurate and validated additional information pertaining to individual customers.</td>
<td>Ability to effectively monitor and detect activities pertaining to ML/TF. • Ability to mitigate the risk of financial or non-financial penalties due to non-compliance imposed by the regulatory authority (cost avoidance).(042; 041; 004; 008) • Ability to mitigate the risk of adverse implications to the image of the organisation (i.e. reputational risk) due to being associated with ML/TF.(039; 006; 003; 034; 008) • Ability to facilitate overseas banking operations (e.g. establishing overseas branches or providing corresponding banking services) by meeting the requirements on AML/CFT.(016) • Ability to ensure that additional and extra information for individual customers is adequately validated and correct.</td>
<td>Opportunity to access additional and extra information on individual customers that could be used to correctly pinpoint targeted customers for business relationship enhancement activities (e.g. cross-selling, differential pricing and promotional campaigns, etc.) at a later period or when the need arises. • Opportunity to increase the productivity and effectiveness of organisation’s business relationship enhancement efforts by having access to validated and accurate information on individual customers. • Opportunity to guide or tailor organisation’s future business relationship enhancement efforts based on information such as customer’s age, occupation,</td>
</tr>
</tbody>
</table>

In addition to the above, other information such as type of occupation; name of employer; nature of business or self-employment; and contact number for home, office or mobile; is also required.
### Appendix VIII

<table>
<thead>
<tr>
<th>No</th>
<th>Required Changes / Actions</th>
<th>Related Sections</th>
<th>Expected Deliverables</th>
<th>Compliance Benefits</th>
<th>Supplementary Benefits</th>
</tr>
</thead>
</table>
|    | CDD for and monitoring of non face-to-face customers should be as effective as face-to-face customers. Reporting institution may use (but not limited to) the following:  
- Request for supplementary documents, over and above the ones required for face-to-face customers  
- Develop independent contact with the customer; or  
- Verify customer details against repositories maintained by authorities. | STG, 5.8.3 & 5.8.4 | Cell 1 | and accurately obtained and validated. | Opportunity to access accurate and validated information on non face-to-face customers that could be used for business relationship enhancement activities at a later period or when the need arises.  
Opportunity to detect genuine customer’s transactions (i.e. false alerts) that could be used to trigger, as well as be an input to business relationship enhancement activities of the organisation.  
Opportunity to increase the productivity and effectiveness of organisation’s business relationship enhancement efforts (i.e. increase the chances of achieving success) by having access to validated and accurate information, as well as by having the ability to detect false alerts for non face-to-face customers. |
| 13 | Establishment of or enhancement to manual policies and procedures on CDD for non face-to-face customers to obtain and verify the required information.  
Establishment of or enhancement to CDD process in the business IT system for non face-to-face customers to obtain and verify the required information.  
Establishment of or enhancement to customer monitoring module in the AML/CFT IT system to detect discrepancies in financial transactions or activities for non face-to-face customers. Key AML/CFT IT system functionalities that would assist in meeting this requirement are:  
- customer due diligence,  
- behaviour profiling, | | Cell 2 | Ability to effectively monitor and detect activities pertaining to ML/TF.  
Ability to mitigate the risk of financial or non-financial penalties due to non-compliance imposed by the regulatory authority (cost avoidance). (042; 041; 004; 008)  
Ability to mitigate the risk of adverse implications to the image of the organisation (i.e. reputational risk) due to being associated with ML/TF. (039; 006; 003; 034; 008)  
Ability to facilitate overseas banking operations (e.g. establishing overseas branches or providing corresponding banking services) by meeting the requirements on AML/CFT. (016)  
Ability to ensure that information for non face-to-face customers is adequately and accurately obtained and validated. |
<table>
<thead>
<tr>
<th>No</th>
<th>Required Changes / Actions</th>
<th>Related Sections</th>
<th>Expected Deliverables</th>
<th>Compliance Benefits</th>
<th>Supplementary Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>Establish a risk management framework to determine whether a customer (new or current) is a Foreign Politically Exposed Person (PEP).&lt;br&gt;• At minimum, appropriate and adequate information from the customer, as well as from information available publicly should be gathered.&lt;br&gt;• If the customer is a PEP, the source of wealth and funds are to be established.&lt;br&gt;• The decision to establish or continue the business relationship with PEPs is to be decided by the senior management at the head office of the reporting</td>
<td>STG, 5.9.3 to 5.9.6; SCG1, 4.6.1</td>
<td>• Establishment of or enhancement to the organisation’s risk management framework for the detection and management of PEPs.&lt;br&gt;• Availability of a report that provide accurate details of customers that have been classified as PEPs.&lt;br&gt;• Availability of exception reports based on discrepancies in financial transactions or activities in contrast to the profile of PEPs.&lt;br&gt;• Establishment of or enhancement to customer monitoring module in the AML/CFT IT system to detect discrepancies in financial transactions or activities for PEPs. Key AML/CFT IT system</td>
<td>• Ability to effectively monitor and detect activities pertaining to ML/TF.&lt;br&gt;• Ability to mitigate the risk of financial or non-financial penalties due to non-compliance imposed by the regulatory authority (cost avoidance). (042; 041; 004; 008)&lt;br&gt;• Ability to mitigate the risk of adverse implications to the image of the organisation (i.e. reputational risk) due to being associated with ML/TF. (039; 006; 003; 034; 008)&lt;br&gt;• Ability to facilitate overseas banking operations (e.g. establishing overseas branches or providing corresponding banking services) by meeting the requirements on AML/CFT. (016)</td>
<td>• Opportunity to mitigate the risk of inadvertently prospecting customers that may turn out to be associated with ML/TF (as the triggering customers’ information is detected from transactions that have been deemed as genuine).&lt;br&gt;• N/A&lt;br&gt;• As the decision to continue the relationship with PEPs will require the senior management approval, any further enhancement to business relationship with PEPs may also likely to require similar level of management approval. Therefore, this will significantly reduce the time-critical advantage of detecting genuine transactions (i.e. false alerts) that could be used to trigger, as well as be an input to business relationship enhancement activities with potential PEPs.&lt;br&gt;• In addition, attaining Supplementary benefit to business by enhancing customer...</td>
</tr>
</tbody>
</table>
### Appendix VIII

<table>
<thead>
<tr>
<th>No</th>
<th>Required Changes / Actions</th>
<th>Related Sections</th>
<th>Expected Deliverables</th>
<th>Compliance Benefits</th>
<th>Supplementary Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>institution.</td>
<td></td>
<td>functionalities that would assist in meeting this requirement are:</td>
<td>Ability to ensure that the accounts of PEPs are examined to detect discrepancies in financial transactions or activities.</td>
<td>relationship with PEPs (which is sensitive and risky in nature) may not be a policy that the organisation wishes to undertake.</td>
</tr>
<tr>
<td>15</td>
<td>Enhanced CDD should be conducted on higher risk customers, such as:</td>
<td>STG, 5.10.1 to 5.10.3</td>
<td>Establishment of or enhancement to manual policies and procedures on enhanced CDD for high risk customers. Establishment of or enhancement to enhanced CDD process in the business IT system for high risk customers. Availability of accurate and validated additional information pertaining to high risk customers.</td>
<td>Ability to effectively monitor and detect activities pertaining to ML/TF. Ability to mitigate the risk of financial or non-financial penalties due to non-compliance imposed by the regulatory authority (cost avoidance). (042; 041; 004; 008) Ability to mitigate the risk of adverse implications to the image of the organisation (i.e. reputational risk) due to being associated with ML/TF. (039; 006; 003; 034; 008) Ability to facilitate overseas banking operations (e.g. establishing overseas branches or providing corresponding banking</td>
<td>Opportunity to access additional and extra information on high risk customers that have business potentials (such as high net worth customers), which could be used for business relationship enhancement activities at a later period or when the need arises. Opportunity to increase the productivity and effectiveness of organisation’s business relationship enhancement efforts by having access to validated and accurate information on high risk customers (i.e. for customers of high net worth).</td>
</tr>
<tr>
<td>No</td>
<td>Required Changes / Actions</td>
<td>Related Sections</td>
<td>Expected Deliverables</td>
<td>Compliance Benefits</td>
<td>Supplementary Benefits</td>
</tr>
<tr>
<td>----</td>
<td>-----------------------------</td>
<td>------------------</td>
<td>-----------------------</td>
<td>---------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td></td>
<td>business; and</td>
<td></td>
<td></td>
<td>service) by meeting the requirements on AML/CFT.(016)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• customers with</td>
<td></td>
<td></td>
<td>Ability to ensure that additional and extra information on high risk customers is adequately and accurately obtained and validated.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>business/activities that are considered having high AML/CFT risk by FATF Enhanced CDD should (at minimum) meet the following:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• obtain detailed information from customer, as well as from information available publicly, especially on the purpose of transaction and source of funds; and</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• obtain senior management approval before the establishment of business relationship.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>CDD on existing customer should ensure that information (including the customer profile) is up-to-date and relevant. This is primarily when:</td>
<td>STG, S.11.1 &amp; S.11.2</td>
<td>• Establishment of or enhancement to manual policies and procedures on maintaining existing customers’ information and profiling to ensure that they are up-to-date and relevant.</td>
<td>• Ability to effectively monitor and detect activities pertaining to ML/TF.</td>
<td>• Opportunity to access accurate and up-to-date customer’s information that could be used to pinpoint customers for business relationship enhancement activities (e.g. cross-selling, differential pricing and promotional campaigns, etc.) at a later period or when the need arises.</td>
</tr>
<tr>
<td></td>
<td>• there is a significant transaction about to occur;</td>
<td></td>
<td>• Establishment of or enhancement to CDD and profiling processes in the business IT system for existing customers to ensure that their information is up-to-date and relevant.</td>
<td>• Ability to mitigate the risk of financial or non-financial penalties due to non-compliance imposed by the regulatory authority (cost avoidance).(042; 041; 004; 008)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• there is a material change on how the account is managed;</td>
<td></td>
<td>• Availability of accurate and up-to-date customer’s information that could be used to pinpoint customers for business relationship enhancement activities (e.g. cross-selling, differential pricing and promotional campaigns, etc.) at a later period or when the need arises.</td>
<td>• Ability to mitigate the risk of adverse implications to the image of the organisation (i.e. reputational risk) due to being associated with ML/TF.(039; 006; 003; 034; 008)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• there is considerable change to the customer's documentation standards;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>Required Changes / Actions</td>
<td>Related Sections</td>
<td>Expected Deliverables</td>
<td>Compliance Benefits</td>
<td>Supplementary Benefits</td>
</tr>
<tr>
<td>----</td>
<td>-----------------------------</td>
<td>------------------</td>
<td>-----------------------</td>
<td>---------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td></td>
<td>or</td>
<td></td>
<td>to-date information on existing customers.</td>
<td>Ability to facilitate overseas banking operations (e.g. establishing overseas branches or providing corresponding banking services) by meeting the requirements on AML/CFT.(016)</td>
<td>by having access to accurate and up-to-date customer’s information. For example, organisations will be able to benefit by ensuring up-to-date customer information is acquired when a significant transaction is about to occur. In this circumstance, the organisation would have the opportunity to leverage the updated customer information for business relationship enhancement purposes, particularly when the expected customer transaction is found to have business benefit properties.</td>
</tr>
</tbody>
</table>
| 17 | Transactions involving wire transfers should require the following:  
   a) If the reporting institution is an ordering institution  
      • Ensure minimum originator information are obtained, i.e. name; nationality; NRIC or passport number; account or unique reference number; and address (or date and place of birth, if address is not available);  
   | SCG1, 4.4.1 to 4.4.7 | Establishment of or enhancement to manual policies and procedures on CDD for wire transfer transactions.  
   | | Establishment of or enhancement to CDD process in the business IT system for wire transfer transactions.  
   | | Establishment of or enhancement to customer monitoring process in the AML/CFT IT system to detect discrepancies in wire transfer transactions. Key AML/CFT IT | Ability to effectively monitor and detect activities pertaining to ML/TF.  
   | | Ability to mitigate the risk of financial or non-financial penalties due to non-compliance imposed by the regulatory authority (cost avoidance).(042; 041; 004; 008)  
   | | Ability to mitigate the risk of adverse implications to the image of the organisation (i.e. reputational risk) due to being associated with ML/TF.(039; 006; 003; 034; 008)  
   | | Opportunity to access accurate and validated customer’s information based on wire transfer transactions that could be used to correctly pinpoint targeted customers for business relationship enhancement activities (e.g. cross-selling, differential pricing and promotional campaigns, etc.) at a later period or when the need arises.  
<p>| | Opportunity to increase the productivity and effectiveness of |</p>
<table>
<thead>
<tr>
<th>No</th>
<th>Required Changes / Actions</th>
<th>Related Sections</th>
<th>Expected Deliverables</th>
<th>Compliance Benefits</th>
<th>Supplementary Benefits</th>
</tr>
</thead>
</table>
|    | • Transmit the name,        |                  | system functionalities that would assist in meeting this requirement are:  
|    | account or unique reference number, and address (or NRIC or passport number or date of birth, if address is not available). |                  | • customer due diligence,  
|    | b) If the reporting institution is acting as an intermediary  
|    | • Ensure that the originator information is retained in the wire transfer message. |                  | • behaviour profiling,  
|    | c) If the reporting institution is a beneficiary institution  
|    | • Should adopt effective risk based approach to detect wire transfer messages that are incomplete or missing, and decide whether to proceed or cease the transaction, or request for the missing information. |                  | • suspicious transactions monitoring,  
|    | Wire transfer messages with incomplete originator’s information may be treated as suspicious and be reported accordingly. |                  | • alert management, and  
|    | Ensures that wire transfers from high risk customers are |                  | • link analysis.  
<p>|    | |                  | • Availability of accurate and validated customers’ information pertaining wire transfer transactions. | | organisation’s business relationship enhancement efforts by having access to accurate and validated information on customers. For example, the ability to accurately identify customers that have conducted wire transfer transactions could be used to correctly analyse and identify customers’ past transactional habits and tendencies to detect any business benefit properties. |
|    | |                  | • Availability of exception reports based on discrepancies in wire transfer transactions. | | |</p>
<table>
<thead>
<tr>
<th>No</th>
<th>Required Changes / Actions</th>
<th>Related Sections</th>
<th>Expected Deliverables</th>
<th>Compliance Benefits</th>
<th>Supplementary Benefits</th>
</tr>
</thead>
</table>
|    | assessed (such as on the name of beneficiary, destination and amount) Request further details on wire transfers that appeared to be inconsistent with the customer’s usual business or activity patterns. | SCG1, 4.10.1 & 4.10.2 | • Establishment of or enhancement to manual policies and procedures on enhanced CDD for private banking customers.  
• Establishment of or enhancement to the business IT system on enhanced CDD for private banking customers.  
• Availability of accurate and validated additional information pertaining to private banking customers.  
• Availability of stringent approval process for private banking customers | • Ability to effectively monitor and detect activities pertaining to ML/TF.  
• Ability to mitigate the risk of financial or non-financial penalties due to non-compliance imposed by the regulatory authority (cost avoidance).(042; 041; 004; 008)  
• Ability to mitigate the risk of adverse implications to the image of the organisation (i.e. reputational risk) due to being associated with ML/TF.(039; 006; 003; 034; 008)  
• Ability to facilitate overseas banking operations (e.g. establishing overseas branches or providing corresponding banking services) by meeting the requirements on AML/CFT.(016)  
• Ability to ensure that information from private banking customers is adequately and accurately | • Even though the number of customers in the private banking category would tend to be smaller to the number of retail customers, the following Supplementary benefits could still be attained by the organisation through the due diligence process established for AML/CFT:  
• Opportunity to access accurate and up-to-date customer’s information that could be used for business relationship enhancement activities (e.g. cross-selling, differential pricing and promotional campaigns, etc.) at a later period or when the need arises.  
• Opportunity to increase the productivity and effectiveness of organisation’s business |
<table>
<thead>
<tr>
<th>No</th>
<th>Required Changes / Actions</th>
<th>Related Sections</th>
<th>Expected Deliverables</th>
<th>Compliance Benefits</th>
<th>Supplementary Benefits</th>
</tr>
</thead>
</table>
| 19 | Due diligence on credit cards with supplementary cardholders associated with a personal card account or employees holding corporate cards should ensure that relevant details of the supplementary cardholders are obtained for identification and verification. The reporting institution should also reasonably ensure that the supplementary cardholders are not listed as terrorists in the list maintained by the United Nations. | SCG1, 4.11.1 & 4.11.2 | - Establishment of or enhancement to manual policies and procedures on CDD for supplementary credit cardholders customers.  
- Establishment of or enhancement to the business IT system on CDD for supplementary credit cardholders customers.  
- Establishment of or enhancement to customer's name filtering module in the AML/CFT IT system. Key AML/CFT IT system functionalities that would assist in meeting this requirement are:  
  - watch list filtering, and  
  - alert management.  
- Availability of accurate and validated additional information pertaining to supplementary credit cardholders customers. | - Ability to effectively monitor and detect activities pertaining to ML/TF.  
- Ability to mitigate the risk of financial or non-financial penalties due to non-compliance imposed by the regulatory authority (cost avoidance).(042; 041; 004; 008)  
- Ability to mitigate the risk of adverse implications to the image of the organisation (i.e. reputational risk) due to being associated with ML/TF.(039; 006; 003; 034; 008)  
- Ability to facilitate overseas banking operations (e.g. establishing overseas branches or providing corresponding banking services) by meeting the requirements on AML/CFT.(016)  
- Ability to ensure accurate and validated supplementary credit cardholder’s name that facilitates effective matching with the list of names that are known to be associated with ML/TF. | - Opportunity to access accurate and validated supplementary credit cardholder’s information that could be used for business relationship enhancement activities (e.g. cross-selling, differential pricing and promotional campaigns, etc.) at a later period or when the need arises.  
- Opportunity to increase the productivity and effectiveness of organisation’s business relationship enhancement efforts by having access to accurate and validated information supplementary credit cardholder customers. |
<table>
<thead>
<tr>
<th>No</th>
<th>Required Changes / Actions</th>
<th>Related Sections</th>
<th>Expected Deliverables</th>
<th>Compliance Benefits</th>
<th>Supplementary Benefits</th>
</tr>
</thead>
</table>
| 20 | The retention period for relevant records (in particular for those obtained during CDD) should be for a minimum of 6 years subsequent to the completed transaction or after the termination of the business relationship with the customer. However, the retention period will be extended (until the records are no longer needed) when they are used for on-going investigation or prosecution in the court of law. | STG, 6.1.1 & 6.1.2; AMLATFA, section 17(1) | • Establishment of or enhancement to manual policies and procedures on retention of records.  
• Establishment of or enhancement to the business IT system, as well as AML/CFT IT system to meet the requirements on retention of records.  
• Availability of historical records of customers for a minimum of 6 years, particularly pertaining to CDD. | • Ability to effectively monitor and detect activities pertaining to ML/TF.  
• Ability to mitigate the risk of financial or non-financial penalties due to non-compliance imposed by the regulatory authority (cost avoidance).(042; 041; 004; 008)  
• Ability to mitigate the risk of adverse implications to the image of the organisation (i.e. reputational risk) due to being associated with ML/TF.(039; 006; 003; 034; 008)  
• Ability to facilitate overseas banking operations (e.g. establishing overseas branches or providing corresponding banking services) by meeting the requirements on AML/CFT.(016)  
• Ability to access minimum of 6 years historical customers’ information for AML/CFT purposes when the need arises. (Underlying Information Architecture) | • N/A. Information on customers is largely pertaining to CDD. |
| 21 | Record kept for the above period should allow for the establishment of audit trail, i.e. the history, circumstances and events, etc. | STG, 6.2.2; AMLATFA, sections | • Establishment of or enhancement to manual policies and procedures on the clarity and comprehensiveness of the information. | • Ability to effectively monitor and detect activities pertaining to ML/TF.  
• Ability to mitigate the risk of financial or non-financial penalties due to non-compliance imposed by the regulatory authority (cost avoidance).(042; 041; 004; 008)  
• Ability to mitigate the risk of adverse implications to the image of the organisation (i.e. reputational risk) due to being associated with ML/TF.(039; 006; 003; 034; 008)  
• Ability to facilitate overseas banking operations (e.g. establishing overseas branches or providing corresponding banking services) by meeting the requirements on AML/CFT.(016)  
• Ability to access minimum of 6 years historical customers’ information for AML/CFT purposes when the need arises. (Underlying Information Architecture) | • N/A. Information on customers is largely pertaining to CDD. |
<table>
<thead>
<tr>
<th>No</th>
<th>Required Changes / Actions</th>
<th>Related Sections</th>
<th>Expected Deliverables</th>
<th>Compliance Benefits</th>
<th>Supplementary Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>13 &amp; 17(2)</td>
<td>Establishment of or enhancement to the business IT system, as well as AML/CFT IT system to meet the clarity and comprehensiveness requirements of records being retained.</td>
<td>records being retained.</td>
<td>financial or non-financial penalties due to non-compliance imposed by the regulatory authority (cost avoidance). (042; 041; 004; 008)</td>
<td>Ability to mitigate the risk of adverse implications to the image of the organisation (i.e. reputational risk) due to being associated with ML/TF. (039; 006; 003; 034; 008)</td>
<td></td>
</tr>
<tr>
<td>13 &amp; 17(2)</td>
<td>Availability of detailed and comprehensive historical customers’ records that allow for the establishment of audit trail.</td>
<td>records being retained.</td>
<td>Ability to mitigate the risk of adverse implications to the image of the organisation (i.e. reputational risk) due to being associated with ML/TF. (039; 006; 003; 034; 008)</td>
<td>Ability to access detailed and comprehensive historical customers records that allow for the establishment of audit trail for AML/CFT purposes when the need arises (such as allowing for the reconstruction of event for presentation of evidence in the court of law). (Underlying Information Architecture)</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Record kept should be secure and retrievable upon request in a timely manner</td>
<td>STG, 6.2.3</td>
<td>Establishment of or enhancement to manual policies and procedures on the safety and timely retrievability of records that are being retained.</td>
<td>Ability to effectively monitor and detect activities pertaining to ML/TF.</td>
<td>Ability to mitigate the risk of financial or non-financial penalties</td>
</tr>
<tr>
<td>22</td>
<td>Record kept should be secure and retrievable upon request in a timely manner</td>
<td>STG, 6.2.3</td>
<td>Establishment of or enhancement to manual policies and procedures on the safety and timely retrievability of records that are being retained.</td>
<td>Ability to effectively monitor and detect activities pertaining to ML/TF.</td>
<td>Ability to mitigate the risk of financial or non-financial penalties</td>
</tr>
<tr>
<td>22</td>
<td>Record kept should be secure and retrievable upon request in a timely manner</td>
<td>STG, 6.2.3</td>
<td>Establishment of or enhancement to manual policies and procedures on the safety and timely retrievability of records that are being retained.</td>
<td>Ability to effectively monitor and detect activities pertaining to ML/TF.</td>
<td>Ability to mitigate the risk of financial or non-financial penalties</td>
</tr>
<tr>
<td>22</td>
<td>Record kept should be secure and retrievable upon request in a timely manner</td>
<td>STG, 6.2.3</td>
<td>Establishment of or enhancement to manual policies and procedures on the safety and timely retrievability of records that are being retained.</td>
<td>Ability to effectively monitor and detect activities pertaining to ML/TF.</td>
<td>Ability to mitigate the risk of financial or non-financial penalties</td>
</tr>
<tr>
<td>22</td>
<td>Record kept should be secure and retrievable upon request in a timely manner</td>
<td>STG, 6.2.3</td>
<td>Establishment of or enhancement to manual policies and procedures on the safety and timely retrievability of records that are being retained.</td>
<td>Ability to effectively monitor and detect activities pertaining to ML/TF.</td>
<td>Ability to mitigate the risk of financial or non-financial penalties</td>
</tr>
<tr>
<td>22</td>
<td>Record kept should be secure and retrievable upon request in a timely manner</td>
<td>STG, 6.2.3</td>
<td>Establishment of or enhancement to manual policies and procedures on the safety and timely retrievability of records that are being retained.</td>
<td>Ability to effectively monitor and detect activities pertaining to ML/TF.</td>
<td>Ability to mitigate the risk of financial or non-financial penalties</td>
</tr>
<tr>
<td>22</td>
<td>Record kept should be secure and retrievable upon request in a timely manner</td>
<td>STG, 6.2.3</td>
<td>Establishment of or enhancement to manual policies and procedures on the safety and timely retrievability of records that are being retained.</td>
<td>Ability to effectively monitor and detect activities pertaining to ML/TF.</td>
<td>Ability to mitigate the risk of financial or non-financial penalties</td>
</tr>
<tr>
<td>22</td>
<td>Record kept should be secure and retrievable upon request in a timely manner</td>
<td>STG, 6.2.3</td>
<td>Establishment of or enhancement to manual policies and procedures on the safety and timely retrievability of records that are being retained.</td>
<td>Ability to effectively monitor and detect activities pertaining to ML/TF.</td>
<td>Ability to mitigate the risk of financial or non-financial penalties</td>
</tr>
<tr>
<td>22</td>
<td>Record kept should be secure and retrievable upon request in a timely manner</td>
<td>STG, 6.2.3</td>
<td>Establishment of or enhancement to manual policies and procedures on the safety and timely retrievability of records that are being retained.</td>
<td>Ability to effectively monitor and detect activities pertaining to ML/TF.</td>
<td>Ability to mitigate the risk of financial or non-financial penalties</td>
</tr>
<tr>
<td>22</td>
<td>Record kept should be secure and retrievable upon request in a timely manner</td>
<td>STG, 6.2.3</td>
<td>Establishment of or enhancement to manual policies and procedures on the safety and timely retrievability of records that are being retained.</td>
<td>Ability to effectively monitor and detect activities pertaining to ML/TF.</td>
<td>Ability to mitigate the risk of financial or non-financial penalties</td>
</tr>
<tr>
<td>No</td>
<td>Required Changes / Actions</td>
<td>Related Sections</td>
<td>Expected Deliverables</td>
<td>Compliance Benefits</td>
<td>Supplementary Benefits</td>
</tr>
<tr>
<td>----</td>
<td>-----------------------------</td>
<td>------------------</td>
<td>-----------------------</td>
<td>---------------------</td>
<td>-------------------------</td>
</tr>
</tbody>
</table>
|    |                             |                  | • Establishment of or enhancement to the business IT system, as well as AML/CFT IT on the safety and timely retrievability of records that are being retained.  
• Availability of historical customers' records that are securely kept and can be retrieved in a timely manner. | due to non-compliance imposed by the regulatory authority (cost avoidance). (042; 041; 004; 008)  
• Ability to mitigate the risk of adverse implications to the image of the organisation (i.e. reputational risk) due to being associated with ML/TF. (039; 006; 003; 034; 008)  
• Ability to facilitate overseas banking operations (e.g. establishing overseas branches or providing corresponding banking services) by meeting the requirements on AML/CFT. (016)  
• Ability to access historical customer’s records that are securely kept, as well as that allow for timely retrievability when the need arises. (Underlying Information Architecture) | N/A. Centralisation of information is largely pertaining to reporting submitted to the regulatory authority. |
| 23 | Establish the centralisation of information collected pursuant to Part IV of AMLATFA.\(^2\) | AMLATFA, section 15 | • Establishment of or enhancement to manual policies and procedures on centralisation of information relating to AML/CFT.  
• Establishment of or enhancement to the | | |

\(^2\) Part IV or AMLATFA relates to the reporting institutions’ obligations to submit reporting to the competent authority (i.e. the central bank).
<table>
<thead>
<tr>
<th>No</th>
<th>Required Changes / Actions</th>
<th>Related Sections</th>
<th>Expected Deliverables</th>
<th>Compliance Benefits</th>
<th>Supplementary Benefits</th>
</tr>
</thead>
</table>
|    |                             |                  | organisation’s IT system (for business, as well as for AML/CFT purposes) to facilitate the centralisation of information.  
• Availability of information relating to AML/CFT that is centrally stored. | avoidance).(042; 041; 004; 008)  
• Ability to mitigate the risk of adverse implications to the image of the organisation (i.e. reputational risk) due to being associated with ML/TF.(039; 006; 003; 034; 008)  
• Ability to facilitate overseas banking operations (e.g. establishing overseas branches or providing corresponding banking services) by meeting the requirements on AML/CFT.(016)  
• Ability to gain easy access to AML/CFT related information that is stored in a central location. (Underlying Information Architecture) |                                                                 |

**On-going Monitoring**

<table>
<thead>
<tr>
<th>No</th>
<th>Required Changes / Actions</th>
<th>Related Sections</th>
<th>Expected Deliverables</th>
<th>Compliance Benefits</th>
<th>Supplementary Benefits</th>
</tr>
</thead>
</table>
| 24 | Conduct on-going CDD to analyse and clarify the economic background and purpose of any transaction or business relationship that are; uncommon or does not have any clear economic purpose or legitimacy, particularly when involving complex and large transactions or customers of higher risk. Detection can be done at the point of customer | STG, 7.1.1 & 7.1.2 | • Establishment of or enhancement to manual policies and procedures on on-going CDD to ensure the legitimacy of customers’ transactions and behaviours.  
• Establishment of or enhancement to the on-going CDD process in the business IT system to cater for transactions occurring at the point of customer contact. | • Ability to effectively monitor and detect activities pertaining to ML/TF.  
• Ability to mitigate the risk of financial or non-financial penalties due to non-compliance imposed by the regulatory authority (cost avoidance).(042; 041; 004; 008)  
• Ability to mitigate the risk of adverse implications to the image of the organisation (i.e. reputational risk) due to being associated with ML/TF. | • Opportunity to detect genuine customer’s transactions (i.e. false alerts) that could be used to trigger, as well as be an input to time-critical event-based business relationship enhancement activities of the organisation.  
• Opportunity to increase the productivity and effectiveness of organisation’s business relationship enhancement efforts |
<table>
<thead>
<tr>
<th>No</th>
<th>Required Changes / Actions</th>
<th>Related Sections</th>
<th>Expected Deliverables</th>
<th>Compliance Benefits</th>
<th>Supplementary Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>contact or through analysing the customer’s transaction activities or patterns.</td>
<td></td>
<td>• Establishment of or enhancement to customer monitoring module in the AML/CFT IT system to detect discrepancies in customers’ financial transactions or activities. Key AML/CFT IT system functionalities that would assist in meeting this requirement are: • customer due diligence, • behaviour profiling, • suspicious transactions monitoring, • alert management, and • link analysis. • Availability of exception reports based on discrepancies in customers’ financial transactions and behaviours against their profiles and economic backgrounds.</td>
<td>associated with ML/TF.(039; 006; 003; 034; 008) • Ability to facilitate overseas banking operations (e.g. establishing overseas branches or providing corresponding banking services) by meeting the requirements on AML/CFT.(016) • Ability to discover and detect discrepancies in customers’ financial transactions or activities against their profiles and economic backgrounds through on-going monitoring.</td>
<td>(i.e. increase the chances of achieving success) by having the ability to detect time-critical event-based customers’ information, discovered through the due diligence process established for AML/CFT. • Opportunity to mitigate the risk of inadvertently prospecting customers that may turn out to be associated with ML/TF (as triggering customers’ information is detected from transactions that have been deemed as genuine).</td>
</tr>
<tr>
<td>25</td>
<td>Establish a Management Information System (MIS) to complement the CDD effort. The MIS should produce timely information on a regular basis to allow for the detection of suspicious activities, which includes; multiple and large transactions; unusual</td>
<td>STG, 7.2.1 &amp; 7.2.2</td>
<td>• Establishment of an IT system for the purpose of timely information, analysis and detection of AML/CFT activities. Key system functionalities that would assist in meeting this requirement are: • customer due diligence, • behaviour profiling,</td>
<td>• Ability to effectively monitor and detect activities pertaining to ML/TF. • Ability to mitigate the risk of financial or non-financial penalties due to non-compliance imposed by the regulatory authority (cost avoidance).(042; 041; 004; 008) • Ability to mitigate the risk of</td>
<td>• Opportunity to timely detect customers’ triggering information (i.e. from the unrestricted false alerts) to act as an input to time-critical event-based business relationship enhancement activities of the organisation. • Opportunity to increase the</td>
</tr>
<tr>
<td>No</td>
<td>Required Changes / Actions</td>
<td>Related Sections</td>
<td>Expected Deliverables</td>
<td>Compliance Benefits</td>
<td>Supplementary Benefits</td>
</tr>
<tr>
<td>----</td>
<td>-----------------------------</td>
<td>------------------</td>
<td>-----------------------</td>
<td>---------------------</td>
<td>------------------------</td>
</tr>
</tbody>
</table>
| 1  | Transaction patterns; or transactions that exceed any internally specified thresholds. The MIS should be part of the bank’s information system that stores accurate and up-to-date customer’s normal transaction or business profile. | • suspicious transactions monitoring,  
• alert management,  
• case management  
• link analysis, and  
• watch list filtering.  
• Availability of information collected from multiple source systems that has been cleansed, in a consistent formatting and stored in a data mart for AML/CFT monitoring, analysis and alert purposes. | adverse implications to the image of the organisation (i.e. reputational risk) due to being associated with ML/TF.(039; 006; 003; 034; 008)  
• Ability to facilitate overseas banking operations (e.g. establishing overseas branches or providing corresponding banking services) by meeting the requirements on AML/CFT.(016)  
• Ability to constantly monitor and provide timely information, analysis, alerts and detection of suspected AML/CFT activities, with drill down capabilities. (016) | productivity and effectiveness of organisation’s business relationship enhancement efforts (i.e. increase the chances of achieving success) by having the ability to timely detect time-critical event-based customers’ information, discovered through the due diligence process established for AML/CFT.  
• Opportunity to mitigate the risk of inadvertently prospecting customers that may turn out to be associated with ML/TF (as triggering customers’ information is detected from transactions that have been deemed as genuine).  
• Opportunity to access for business purposes, information that has been sourced from multiple IT systems, which has been cleansed, in a consistent formatting and is centrally located in a data mart established for regulatory purposes (030).  
• Opportunity for business departments to access cleansed and centrally located information for a wider number of banking |
<table>
<thead>
<tr>
<th>No</th>
<th>Required Changes / Actions</th>
<th>Related Sections</th>
<th>Expected Deliverables</th>
<th>Compliance Benefits</th>
<th>Supplementary Benefits</th>
</tr>
</thead>
</table>
| 26 | Establish internal criteria to monitor and detect unusual or potentially suspicious transactions (red flags). Transactions that match the red flags criteria should be subjected to enhance due | STG, 7.3.1 | • Establishment of or enhancement to manual policies and procedures on monitoring and detection criteria for AML/CFT red flags.  
• Establishment of or enhancement to the business | • Ability to effectively monitor and detect activities pertaining to ML/TF.  
• Ability to mitigate the risk of financial or non-financial penalties due to non-compliance imposed by the regulatory authority (cost | • Opportunity to utilise the enhance due diligence and continuous monitoring mechanisms to discover genuine customer’s transactions (i.e. false alerts) that could be used to trigger, as well as be an input to products (e.g. loans, credit cards, fixed deposits, auto finance, insurance and stock broking – and not being limited to current and savings accounts only. (003; 034)  
• Opportunity to enhance the efficiency of organisation’s IS operations by allowing other departments to increase their turnaround time by acquiring the needed information directly from the AML/CFT data mart (i.e. rather than obtaining directly from the various source systems and undergoing labourious cleansing and formatting process). (037; 018; 034)  
• Opportunity to reduce the risk or safeguard organisational profit against financial losses due to fraud occurrences by leveraging fraud monitoring capabilities in the AML/CFT IT system (001). |
<table>
<thead>
<tr>
<th>No</th>
<th>Required Changes / Actions</th>
<th>Related Sections</th>
<th>Expected Deliverables</th>
<th>Compliance Benefits</th>
<th>Supplementary Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>diligence and on-going monitoring processes.</td>
<td></td>
<td>and the AML/CFT IT systems to cater for the monitoring and detection criteria for AML/CFT red flags. Key AML/CFT IT system functionalities that would assist in meeting this requirement are: • suspicious transactions monitoring, and • alert management. • Availability of exception reports based on triggered red flags (i.e. arising from unusual or potentially suspicious customers’ transactions) that are subjected to enhance due diligence and on-going monitoring processes.</td>
<td>avoidance). (042; 041; 004; 008) • Ability to mitigate the risk of adverse implications to the image of the organisation (i.e. reputational risk) due to being associated with ML/TF. (039; 006; 003; 034; 008) • Ability to facilitate overseas banking operations (e.g. establishing overseas branches or providing corresponding banking services) by meeting the requirements on AML/CFT. (016) • Ability to discover and detect unusual or potentially suspicious customers’ transactions.</td>
<td>time-critical event-based business relationship enhancement activities of the organisation. • Opportunity to increase the productivity and effectiveness of organisation’s business relationship enhancement efforts (i.e. increase the chances of achieving success) by having the ability to detect time-critical event-based customers’ information, discovered through the due diligence process established for AML/CFT. • Opportunity to mitigate the risk of inadvertently prospecting customers that may turn out to be associated with ML/TF (as triggering customers’ information is detected from transactions that have been deemed as genuine).</td>
</tr>
<tr>
<td>27</td>
<td>Conduct on-going due diligence and monitoring of transactions for individuals and business entities that originated from countries that have been deemed to have insufficient AML/CFT measures by internationally recognised</td>
<td>STG, 7.3.2</td>
<td>• Establishment of or enhancement to manual policies and procedures on on-going CDD and monitoring for individuals and business entities that originated from countries that have been deemed to have insufficient AML/CFT measures</td>
<td>• Ability to effectively monitor and detect activities pertaining to ML/TF. • Ability to mitigate the risk of financial or non-financial penalties due to non-compliance imposed by the regulatory authority (cost avoidance). (042; 041; 004; 008)</td>
<td>• Even though the number of foreign customers tend to be smaller as compared with the number of domestic customers, the following Supplementary benefits could still be attained by the organisation through the on-going due diligence and</td>
</tr>
<tr>
<td>No</td>
<td>Required Changes / Actions</td>
<td>Related Sections</td>
<td>Expected Deliverables</td>
<td>Compliance Benefits</td>
<td>Supplementary Benefits</td>
</tr>
<tr>
<td>----</td>
<td>-----------------------------</td>
<td>------------------</td>
<td>-----------------------</td>
<td>---------------------</td>
<td>------------------------</td>
</tr>
</tbody>
</table>
|    | AML/CFT bodies (such as FATF). Detailed further enquiries are required on the background and purpose of the transactions or business relationship. | by internationally recognised AML/CFT bodies.  
- Establishment of or enhancement to the AML/CFT IT system to perform on-going CDD and monitoring for individuals and business entities that originated from countries that are deemed to have insufficient AML/CFT measures by internationally recognised AML/CFT bodies. Key AML/CFT IT system functionalities that would assist in meeting this requirement are:  
  - customer due diligence,  
  - behaviour profiling,  
  - suspicious transactions monitoring,  
  - alert management, and  
  - link analysis.  
- Availability of exception reports on individuals and business entities that originated from countries that have been deemed to have insufficient AML/CFT measures, which will be subjected to on-going due diligence and monitoring.  
- Availability of additional information pertaining to the | • Ability to mitigate the risk of adverse implications to the image of the organisation (i.e. reputational risk) due to being associated with ML/TF. (039; 006; 003; 034; 008)  
• Ability to facilitate overseas banking operations (e.g. establishing overseas branches or providing corresponding banking services) by meeting the requirements on AML/CFT. (016)  
• Ability to discover and detect individuals and business entities that originated from countries that have been deemed to have insufficient AML/CFT measures, which will be subjected to on-going due diligence and monitoring. | monitoring processes established for AML/CFT:  
• Opportunity to access additional and extra information on foreign customers that could be used for business relationship enhancement activities (e.g. differential pricing and promotional campaigns, etc.) at a later period or when the need arises.  
• Opportunity to increase the productivity and effectiveness of organisation’s business relationship enhancement efforts by having access to additional and extra customers’ information.
<table>
<thead>
<tr>
<th>No</th>
<th>Required Changes / Actions</th>
<th>Related Sections</th>
<th>Expected Deliverables</th>
<th>Compliance Benefits</th>
<th>Supplementary Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>background and purpose of the transactions or business relationship for the identified individuals or business entities.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 28 | Establish a database of names and particulars of terrorist as per the UN Consolidated List and other recognised list of designated individuals or entities. In addition, the database should also include orders that may be issued by the Minister of Home Affairs under sections of 66B and 66C of the AMLATFA. | STG, 9.3         | • Establishment of or enhancement to the AML/CFT IT system to include a database of names and particulars of terrorists, designated individuals or entities that are linked with terrorism financing. | • Ability to effectively monitor and detect activities pertaining to ML/TF. | • By having the database to detect suspected terrorists, organisation would be have the opportunity to:  
  • Select desired and reject undesired new customers through AML/CFT name screening process during opening of new banking account or establishing new banking relationship.(039; 042; 006; 003; 019);  
  • Terminate undesired existing customer relationships that have been detected and suspected to be linked to terrorism.(039; 042; 006; 003; 019); and  
  • Focus the organisation’s effort to enhance business relationship with valued (i.e. residual) customers that have been retained once relationships with undesired customers (and suspected terrorist) are ceased. (042) | • Ability to mitigate the risk of financial or non-financial penalties due to non-compliance imposed by the regulatory authority (cost avoidance).(042; 041; 004; 008)  
• Ability to mitigate the risk of adverse implications to the image of the organisation (i.e. reputational risk) due to being associated with ML/TF.(039; 006; 003; 034; 008)  
• Ability to facilitate overseas banking operations (e.g. establishing overseas branches or providing corresponding banking services) by meeting the requirements on AML/CFT.(016)  
• Ability to detect individuals that are suspected to be terrorists or entities that are linked with terrorism financing.(Underlying Information Architecture) |
<table>
<thead>
<tr>
<th>No</th>
<th>Required Changes / Actions</th>
<th>Related Sections</th>
<th>Expected Deliverables</th>
<th>Compliance Benefits</th>
<th>Supplementary Benefits</th>
</tr>
</thead>
</table>
| 29 | Ensure that the database is up-to-date and relevant and made easily accessible to the employees for the purpose of detecting suspicious transactions. | STG, 9.4 | • Establishment of or enhancement to the AML/CFT IT system to ensure the database of names and particulars of terrorists, designated individuals or entities are constantly up-to-date and easily accessible to related employees. | • Ability to effectively monitor and detect activities pertaining to ML/TF.  
• Ability to mitigate the risk of financial or non-financial penalties due to non-compliance imposed by the regulatory authority (cost avoidance).(042; 041; 004; 008)  
• Ability to mitigate the risk of adverse implications to the image of the organisation (i.e. reputational risk) due to being associated with ML/TF.(039; 006; 003; 034; 008)  
• Ability to facilitate overseas banking operations (e.g. establishing overseas branches or providing corresponding banking services) by meeting the requirements on AML/CFT.(016)  
• Ability to ensure the efficiency and effectiveness of AML/CFT detection by providing up-to-date and readily accessible database to related employees.(Underlying Information Architecture) | • By having an up-to-date and readily accessible database on suspected terrorists, organisation would be have the opportunity to:  
• Select desired and reject undesired new customers through AML/CFT name screening process during opening of new banking account or establishing new banking relationship.(039; 042; 006; 003; 019);  
• Terminate undesired existing customer relationships that have been detected and suspected to be linked to terrorism.(039; 042; 006; 003; 019); and  
• Focus the organisation’s effort to enhance business relationship with valued (i.e. residual) customers that have been retained once relationships with undesired customers (and suspected terrorist) are ceased. (042) |
| 30 | Conduct regular assessments on customers’ names (new or existing) against the information in the database. | STG, 9.5 | • Establishment of or enhancement to organisation’s policies and procedures to ensure continuous reviews on | • Ability to effectively monitor and detect activities pertaining to ML/TF.  
• Ability to mitigate the risk of | • Opportunity to select desired and reject undesired new customers through AML/CFT name screening process during |
<table>
<thead>
<tr>
<th>No</th>
<th>Required Changes / Actions</th>
<th>Related Sections</th>
<th>Expected Deliverables</th>
<th>Compliance Benefits</th>
<th>Supplementary Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Any name match should be followed by reasonable and proper verification to confirm the identity, and subsequently the reporting institution should:</td>
<td></td>
<td>customers’ names against the information in the database of names and particulars of terrorists, designated individuals or entities that are linked with terrorism financing.</td>
<td>financial or non-financial penalties due to non-compliance imposed by the regulatory authority (cost avoidance). (042; 041; 004; 008)</td>
<td>opening of new banking account or establishing new banking relationship. (039; 042; 006; 003; 019);</td>
</tr>
<tr>
<td></td>
<td>- Inform the FIU; Securities Commission or Labuan Offshore Financial Services Authority (whichever appropriate);</td>
<td></td>
<td>Establishment of or enhancement to the AML/CFT IT system to facilitate continuous reviews on customers’ names against the information in the database of names and particulars of terrorists, designated individuals or entities that are linked with terrorism financing.</td>
<td>Ability to mitigate the risk of adverse implications to the image of the organisation (i.e. reputational risk) due to being associated with ML/TF. (039; 006; 003; 034; 008)</td>
<td>- Opportunity to terminate undesired existing customer relationships that have been detected and suspected to be linked to terrorism (039; 042; 006; 003; 019); and</td>
</tr>
<tr>
<td></td>
<td>- Reject the (new) customer’s transaction or freeze the (existing) customer’s transaction; and</td>
<td></td>
<td>Key AML/CFT IT system functionalities that would assist in meeting this requirement are:</td>
<td>Ability to facilitate overseas banking operations (e.g. establishing overseas branches or providing corresponding banking services) by meeting the requirements on AML/CFT. (016)</td>
<td>- Opportunity to focus the organisation’s effort to enhance business relationship with valued (i.e. residual) customers that have been retained once relationships with undesired customers (and suspected money launderers) are ceased. (042)</td>
</tr>
<tr>
<td></td>
<td>- Submit STR to FIU if the transaction is suspected to be terrorist related.</td>
<td></td>
<td>• suspicious transactions monitoring,</td>
<td>Ability to detect individuals that are suspected to be terrorists or entities that are linked with terrorism financing.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• alert management, and</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• watch list filtering.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Availability of exception reports on individuals that are suspected terrorists or entities that are suspected to be linked with terrorism financing.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix IX: Additional Sections Necessitating Effective CDD Process

(for specific type of banking customers and transactions)

a) The due diligence process on *individual customers* should at minimum require information in the form of customer’s full name; the NRIC (National Registration Identity Card) or passport number; permanent and correspondence addresses; as well as date of birth and nationality [STG, section 5.2.1]. In addition, the due diligence process should also prompt for any other customer’s official identification documents whenever there is any doubt on the authenticity of the customer’s identity [STG, section 5.2.3]. Furthermore, in specific relation to the banking industry (as outlined in SCG1), supplementary information, such as type of occupation; name of employer; nature of business or self-employment; and contact phone number for home, office or mobile are to be obtained as well [SCG1, section 4.2.1];

b) The due diligence process for organisation’s *non face-to-face customers* is expected to be as effective as the one established for its face-to-face customers. For example, organisations may (but not limited to) request for supplementary documents, over and above the ones required for face-to-face customers. In addition, organisations may also develop an independent contact with the customer or verify customer details against repositories maintained by the authorities [STG, sections 5.8.3 and 5.8.4];

c) An enhanced customer due diligence is required to be conducted on organisation’s *higher risk customers* [STG, section 5.10.1]. The enhanced customer due diligence process should at minimum ensure that detailed information is obtained from the customers themselves, as well as from what is available in the public domains, particularly in determining the purpose of transactions and the sources of funds. Furthermore, approval from the organisation’s senior management should also be obtained prior to establishing a business relationship with this type of customers [STG, section 5.10.2];

d) Organisations are required to obtain explicit customer information when they are acting as an ordering institution in a *wire transfers transactions*. In this
c) In this circumstance, the organisation needs to ensure that minimum originator’s information is obtained, i.e. the name; nationality; NRIC or passport number; account or unique reference number; and address (or date and place of birth, if address is not available) [SCG1, section 4.4.1]. In contrast, in the occasion when the organisation is to act as a beneficiary institution in a wire transfer transaction, it needs to adopt an effective risk based approach to detect wire transfer messages that are incomplete or missing, and decide whether to proceed or cease the transaction, or request for the missing information to be furnished [SCG1, section 4.4.4]. Furthermore, it is also required that the organisation ensures that wire transfers from customers that have been deemed as high risk customers to be scrutinised, such as on the name of beneficiary, the destination, as well as the amount that being transferred [SCG1, section 4.4.6];

e) Enhanced due diligence and more stringent approval process should be deployed prior to engaging any individuals in private banking business relationship [SCG1, section 4.10.1]. In addition, an independent review of the conduct and development the business relationship with private banking customers should be done at least on annual basis [SCG1, section 4.10.2]; and

f) The due diligence process should also be conducted on credit cards customers with supplementary cardholders associated with a personal card account or employees holding corporate cards. In this circumstance, organisations need to ensure that relevant details of the supplementary cardholders are obtained for identification and verification purposes [SCG1, section 4.11.1].
Appendix X: Requirements to Obtain and Maintain Customer Information

a) The need to obtain adequate evidence and accurately establish individual’s identity and legal existence when a customer aspires to commence a business relationship with the bank. All evidences authenticating the status of the customer should be supported by reliable and independent source documents [STG, section 5.1.1; AMLATFA, sections 16(2)(a) and (b)];

b) The need to ensure that customer accounts are maintained in the account holder’s name, and the name used is not anonymous; fictitious; false or incorrect [AMLATFA, sections 16(1)(a) and (b), and section 18 (1)];

c) The need to accurately identify and verify the customer; as well as identify and verify the transaction’s beneficial ownership and control (i.e. the individual or party who ultimately owns or controls the customer’s transaction, especially when there is any suspicion that the transaction is conducted on behalf of a beneficial owner). In addition, the purpose and intention of the business relationship or transaction need to be ascertained; and to ensure that information provided is continuously updated and relevant [STG, section 5.1.3 and 5.6.1; and AMLATFA, sections 16(2)(a) and (b) and section 16 (3)];

d) The need to be aware that the extent of customers’ information required during identification stage would depends on; the risk of money laundering and terrorism financing (ML/TF) based on the customer background and the situation pertaining to the transaction that could be seen as suspicious; the type or form of transaction, and whether it involves a new product or service, or utilising new technology; and the customer’s type (either account holders or non-account holders) and which entities they represent [SCG1, section 4.1.1];

e) The need to maintain the currency and relevancy of existing customers information (including customer profile), especially when; a significant transaction is about to occur; a material change has occurred on how the account is managed; a considerable change to the customer’s documentation standards; or customer’s information is considered insufficient [STG, sections 5.11.1 and 5.11.2];
f) The need to obtain, at minimum, detailed information, as well as information available publicly (especially regarding the purpose of transaction and source of funds) from high risk customers during an enhance CDD process [STG, sections 5.10.1 to 5.10.3];

g) The need to obtain, at minimum; customer’s full name; NRIC (National Registration Identity Card) or passport number; permanent and correspondence addresses; as well as date of birth and nationality, when conducting CDD on an individual customers [STG, section 5.2.1]. In addition, any other customer’s official identification documents should also be required whenever the authenticity of customer’s identity is doubted [STG, section 5.2.3]. Furthermore, information such as type of occupation; name of employer; nature of business or self-employment; and home, office or mobile phone number are likewise to be obtained as well (i.e. in specific relation to the banking industry, as stated in SCG1) [SCG1, section 4.2.1];

h) The need to ensure that non face-to-face customers authentication is as effective as the one deployed for organisation’s face-to-face customers. Supplementary documents, in addition to the ones required for face-to-face customers, may (but not limited to) be requested. Furthermore, an independent contact with the customer can also be established to assist in the authentication process, or to be done through matching of customer details with information in repositories maintained by the authorities [STG, sections 5.8.3 and 5.8.4];

i) The need to obtain relevant details from supplementary credit cardholders (which are associated with personal card or corporate card accounts) for identification and verification purposes, as well as to reasonably ensure that they are not listed as terrorists in the list maintained by the United Nations [SCG1, sections 4.11.1 and 4.11.2];

j) The need to obtain minimum originator’s information, i.e. name; nationality; NRIC or passport number; account or unique reference number; and address (or date and place of birth, if address is not available) when organisations are acting as an ordering institution in a wire transfers transactions [SCG1, section 4.4.1]. In addition, wire transfers from high risk customers need to be scrutinised, such as
on the name of beneficiary, the destination, as well as the amount that being transferred [SCG1, section 4.4.6]. Further details are also needed for wire transfers found to be inconsistent with the customer’s usual business or activity patterns [SCG1, section 4.4.7];

k) The need to deploy a more stringent approval process prior to engaging any individuals in private banking business relationship [SCG1, section 4.10.1]; and

l) The need to ascertain the background and purpose of the financial transactions or business relationship intentions from customers that originated from countries that are considered to have insufficient AML/CFT measures by internationally recognised AML/CFT bodies (such as FATF) [STG, section 7.3.2].
Appendix XI: Overview on Analysis of Capabilities

<table>
<thead>
<tr>
<th>Category</th>
<th>Name</th>
<th>Influence Compliance Benefits?</th>
<th>Influence Supplementary Benefits? (related section(^3))</th>
<th>Improved Competitive Positioning?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outside-in</td>
<td>External relationship management (ERM)</td>
<td>Yes. (all compliance benefits).</td>
<td>Yes. (7.4.1)</td>
<td>No.</td>
</tr>
<tr>
<td></td>
<td>Market responsiveness (MR)</td>
<td>Yes. (all compliance benefits).</td>
<td>No.</td>
<td>No.</td>
</tr>
<tr>
<td>Inside-out</td>
<td>IS infrastructure (ISI)</td>
<td>Yes. (all compliance benefits).</td>
<td>Yes. (7.5.1) (Also; 7.2.1; 7.2.2; 7.3.1; 7.4.1; and 7.6.1)</td>
<td>Yes.</td>
</tr>
<tr>
<td></td>
<td>IS technical skills (ISTS)</td>
<td>No.</td>
<td>No.</td>
<td>No.</td>
</tr>
<tr>
<td></td>
<td>IS development (ISD)</td>
<td>Yes. (all compliance benefits).</td>
<td>No.</td>
<td>No.</td>
</tr>
<tr>
<td></td>
<td>Cost-effective IS operations (CEISO)</td>
<td>Yes. (all compliance benefits).</td>
<td>Yes. (7.5.1)</td>
<td>Yes.</td>
</tr>
<tr>
<td>Spanning</td>
<td>IS-business partnerships (ISBP)</td>
<td>Yes. (all compliance benefits).</td>
<td>No.</td>
<td>No.</td>
</tr>
<tr>
<td></td>
<td>IS planning and change management (ISPCM)</td>
<td>No.</td>
<td>No.</td>
<td>No.</td>
</tr>
<tr>
<td>Supplementary</td>
<td>Compliance – business partnerships (CBP)</td>
<td>Yes. (all compliance benefits).</td>
<td>Yes. (7.5.1; and 7.6.1)</td>
<td>Yes.</td>
</tr>
<tr>
<td></td>
<td>Business knowledge (BK)</td>
<td>Yes. (all compliance benefits).</td>
<td>Yes. (7.6.1)</td>
<td>Yes.</td>
</tr>
<tr>
<td></td>
<td>Analytical and investigation skills (AIS)</td>
<td>Yes. (all compliance benefits).</td>
<td>Yes. (7.6.1)</td>
<td>Yes.</td>
</tr>
</tbody>
</table>

\(^3\) The numbers in parentheses are referring to the relevant sections in Chapter 7